Avaya Integrated Management 3.0

SMON Manager User Guide

14-300209

Issue 2

June 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

*** Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities. Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Table of Contents

Preface . . . . . ***ix***

The Purpose of This Guide ix
Who Should Use This Guide ix
Organization of This Guide ix

Chapter 1 — Overview ***1***

What is RMON 1
What is SMON 2
Switch Monitoring 3
Enterprise Monitoring 3
SMON Management Applications 3
Overview of SMON Concepts 4
SMON Devices 5
Top-Down Monitoring 6
Top-Down Monitoring for the MAC Layer 6
Top-Down Monitoring for the Upper Layers 7
SMON Tools 9
Avaya SMON Manager Tools 10
Enterprise Switch Statistics 10
Enterprise Port Statistics 11
Enterprise Voice Port Statistics 11
Enterprise History 11
Enterprise Switch History 12
Port History 13
Device SMON Tools 14

Chapter 2 — Introduction to Avaya SMON Manager ***15***

Starting Avaya SMON Manager 15
The Online SMON User Interface 15
SMON Tabs 16
Online SMON Toolbar 16
Dialog Area 17
Desktop 17
Working with SMON Tools 18
Configuring Display Options 19
Polling Interval 19
Display Mode 20
Items Per Screen 20
TopN Number of Elements 20

Configuring Report Options 21
Using Dialog Box Options 21
Generating Reports 22
Report Now 23
Auto Report 24
Managing Windows 25

Chapter 3 — Switch Statistics 27

Accessing Switch Statistics 27
Using Switch Statistics 28
Understanding the Switch Statistics Window 28
Selecting Switches to Poll 30
Filtering the Switch Statistics Display 32
Switch Statistics Counters 32
Sorting the Display 33
Searching for Switches 34

Chapter 4 — Port Statistics 35

Accessing Port Statistics 35
Using Port Statistics 36
Understanding the Port Statistics Window 36
Selecting Ports and LAGs to Poll 38
Filtering the Port Statistics Display 40
VLAN Filtering 41
TopN Filtering 42
Port Statistics Counters 43
Sorting the Display 44
Searching for Ports and LAGs 45

Chapter 5 — Voice Port Statistics 47

Accessing Voice Port Statistics 47
Using Voice Port Statistics 48
Understanding the Voice Port Statistics Window 48
Selecting IP Telephones to Poll 50
Filtering the Voice Port Statistics Display 52
Voice Port Statistics Counters 53
Sorting the Display 54
Searching for IP Telephones 55

Chapter 6 — Introduction to SMON History 57

Accessing SMON History 57
The SMON History User Interface 57
SMON Tabs 58
SMON History Toolbar 58
Desktop 59
Info Box 59

Managing Windows 60
History Text Report 60

Chapter 7 — Using SMON History 61

Using Enterprise History 62
Understanding the Enterprise History Window 62
Collection Parameters 65
Activating/Deactivating History Collections 65
Activating Auto Save 66
Viewing the Collection Log 67
Refreshing the Device List 68
Saving the Enterprise History Window 69
Using Switch History 70
Opening a Switch History Window 70
Understanding the Switch History Window 71
Saving a Switch History Report 73
Using Port History 74
Opening the Port History Chart 74
Understanding the Port History Chart 75
Modifying the Port History Display 76

Appendix A — Avaya SMON Manager Menus 77

Online SMON Menus 77
File Menu 77
Edit Menu 77
View Menu 78
Window Menu 78
Help Menu 79
SMON History Menus 79
File Menu 79
Edit Menu 79
View Menu 80
Actions Menu 80
Window Menu 80
Help Menu 81

Appendix B — Setting Up the SMON License 83

Index 85

Preface

Welcome to Avaya SMON Manager. This chapter provides an introduction to the structure and assumptions of the guide. It includes the following sections:

- **The Purpose of This Guide** - A description of the intended purpose of this guide.
- **Who Should Use This Guide** - A description of the intended audience of this guide.
- **Organization of This Guide** - A brief description of the subjects covered in each chapter of this guide.

The Purpose of This Guide

This guide contains the information needed to operate Avaya SMON Manager efficiently and effectively.

Who Should Use This Guide

This guide is intended for use by network managers familiar with network management and its fundamental concepts. It is assumed that the user has the basic responsibility for monitoring Avaya's intelligent switching devices and the network traffic.

Organization of This Guide

This guide is structured to reflect the following conceptual divisions:

- **Introduction** - An introduction to Avaya SMON Manager including the following chapters:
  - **Preface** - This chapter describes the guide's purpose, intended audience, and organization.

  - **Overview** - This chapter provides an overview of the RMON standard and Avaya Inc.'s SMON concepts, a graphical example of SMON's position in a network, a description of the Avaya Inc. switch architecture and monitoring concepts, and an introduction to the SMON tools.

- **Online SMON** - Instructions on how to use Online SMON Manager applications.

  - **Introduction to Avaya SMON Manager** - This chapter describes how to launch Avaya SMON Manager and the SMON tools. It also describes the Online SMON user interface.

  - **Enterprise Switch Statistics** - This chapter describes the Enterprise Switch Statistics tool in detail, including sample screens and filtering options.

  - **Enterprise Port Statistics** - This chapter describes the Enterprise Port Statistics tool in detail, including sample screens and filtering options.

  - **Enterprise Voice Port Statistics** - This chapter describes the Enterprise Voice Port Statistics tool in detail, including sample screens and filtering options.

- **SMON History** - Instructions on how to use SMON History.

  - **Introduction to SMON History** - This chapter explains how to open SMON History and provides a detailed description of the SMON History user interface.

  - **Using SMON History** - This chapter describes the SMON History tools in detail.

The following Appendices are included at the end of this guide:

- **Appendix A** - The full menu structure in Avaya SMON Manager.

- **Appendix B** - How to set up the Avaya SMON Manager license.

1 Overview

This chapter describes Avaya SMON Manager, Avaya Inc.'s switched network monitoring system, and includes the following sections:

- **What is RMON** - A brief description of the RMON standard.
- **What is SMON** - A general description of SMON switch monitoring technology.
- **Overview of SMON Concepts** - An introduction to SMON concepts.
- **SMON Tools** - An introduction to different types of SMON tools.

What is RMON

RMON is the internationally recognized and approved standard for detailed analysis of shared Ethernet and Token Ring media. It ensures consistency in the monitoring and display of statistics between different vendors.

RMON's advanced remote networking capabilities provide the tools needed to monitor and analyze the behavior of segments on a network. In conjunction with an RMON agent, RMON gathers details and logical information about network status, performance, and users running applications on the network.

An RMON agent is a probe that collects information about segments, hosts, and traffic, and sends it to a management station.

The network administrator uses software tools to view the information collected by the RMON agent on the management station.

RMON has two levels:

- RMON I analyzes the MAC layer (Layer 2 in the OSI seven-layer model).
- RMON II analyzes the upper layers (Layers 3 and above).

RMON is an industry standard that Avaya Inc. and other companies have adopted in their network management applications. Avaya has taken the RMON standard and extended it to the switching environment.

What is SMON

SMON is an extension of the RMON standard. SMON adds to the monitoring capabilities of RMON in the following ways:

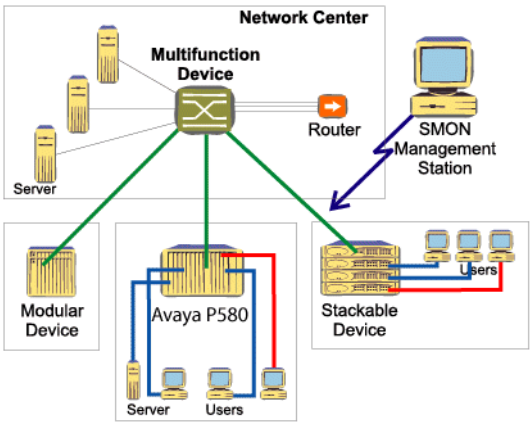
- It provides additional tools and features for monitoring in the switch environment.
- It provides a global view of traffic flow in a network with multiple switches.

SMON extends both RMON I for the MAC layer, and RMON II for the network layer and above. SMON monitoring collects and displays data in real-time.

Using SMON monitoring, you can get:

- A global view of traffic for all switches on the network.
- An overall view of traffic passing through a specific switch.
- Detailed data about the hosts transmitting packets or cells through a switch.
- An analysis of traffic passing through each port connected to a switch.
- A view of traffic between various hosts connected to a switch.

Figure 1-1. SMON Monitoring



Switch Monitoring

Effective switch management requires a comprehensive monitoring mechanism. RMON monitoring is not sufficient for switches. RMON probes can only be used to monitor and analyze a single segment. When you deploy a switch in the network, there are additional components in the network that can not be monitored using RMON, such as switch ports, VLAN, and statistics for all ports.

SMON meets this challenge by extending RMON to the switched network. The SMON extensions of RMON allow the network administrator to analyze the switched network and all of its components.

Enterprise Monitoring

Switches are often used in networks with a complex topology. Switches are typically deployed at the center of an enterprise network between clients and servers, or in backbones to provide high bandwidth and secure connectivity.

Avaya SMON Manager uses a client/server architecture for enterprise monitoring.

SMON extends RMON to provide global monitoring for complex networks. Avaya SMON Manager tools provide a network-wide view of all switched devices in the network. They enable you to monitor the entire network in a single window.

SMON Management Applications

The management applications provided by the SMON extension of RMON include SMON I tools on the MAC layer, and AnyLayer SMON tools on the network layer and above.

The SMON I tools extend RMON I to provide switch monitoring and global network monitoring on the MAC layer. These tools include:

- Enterprise Switch Statistics
- Enterprise Port Statistics
- Enterprise History
- Switch Statistics
- Switch-wide Quality of Service (QoS) indication (provided as part of Switch Statistics)

- VLAN Statistics
- Port Statistics
- Extended Port Statistics
- Ethernet Segment Statistics
- Host Statistics
- Host Matrix Statistics
- Port History

The AnyLayer SMON tools extend RMON II to provide switch monitoring on the network layer and above. These tools include:

- Protocol Directory
- Protocol Distribution
- Network Layer Host Statistics over IP
- Network Layer Subnet Statistics over IP

Overview of SMON Concepts

The SMON applications include Avaya SMON Manager and Avaya Device SMON applications for Avaya Campus devices. These applications comprise an RMON-compliant network management suite that implements the SMON extensions to RMON. Avaya SMON Manager and Avaya Device SMON applications work with the other components of Avaya Network Management to provide a full spectrum of in-depth monitoring of switch traffic and network performance.

Avaya SMON Manager and Avaya Device SMON applications consist of a software console application on a workstation and remote monitoring probes in network devices that support SMON.

The console applications communicate constantly with the SMON devices on your network. The console uses the SNMP protocol to gather information from the devices. Avaya SMON Manager and Avaya Device SMON applications provide you with a suite of powerful graphic display tools to view this information.

Avaya's SMON tools give you detailed analysis of the traffic flow on your switched network, from a global view down to a specific host, and from total MAC layer traffic down to a specific application protocol - all in real-time.

SMON Devices

Avaya's SMON tools provide monitoring capabilities for network devices that support the SMON extensions of the RMON standard.

For Avaya M770, Avaya P130, Avaya C360, Avaya W310, Avaya G250, Avaya G250-BRI, Avaya G350, and Avaya P330 Devices, SMON monitoring capabilities can be activated by purchasing an SMON license from Avaya Inc.

Avaya M770 M-MLS Devices and Avaya P333R Devices also support the AnyLayer SMON extensions of RMON II.

The following table shows the SMON monitoring components supported by the various network devices.

Table 1-1. SMON Monitoring Support by SMON Devices

	Avaya P330 Devices	**Avaya M770 Device DomainX**	**Avaya P460, P580, P882, W310, C360, G250, G350, G250-BRI and P130 Devices**
Enterprise Switch Statistics	√	√	√
Enterprise Port Statistics	√	√	√
Enterprise Voice Port Statistics	√		
Enterprise Port History		√	√
Switch Statistics	√	√	√
Switch-wide QoS Indication		√[1]	
VLAN Statistics	√	√	√
Port Statistics	√[2]	√	√[2]
Ethernet Segment Statistics		√	√
Host Statistics	√[4]		
Host Matrix Statistics	√[4]		
Port History	√	√	√
Protocol Directory	√[4]	√[3]	
Protocol Distribution	√[4]	√[3]	
Network Layer Host Statistics (IP)		√[3]	
Network Layer Subnet Statistics (IP)	√[4]	√[3]	

[1]As part of Switch Statistics application.

[2]Extended Port Statistics are also supported.

[3]Supported when using the Avaya M770 M-MLS.

[4]Supported when using a Avaya P333R module.

Top-Down Monitoring

Avaya's SMON applications provide multi-tiered monitoring capabilities, both for the MAC layer (SMON I) and for upper layers (AnyLayer SMON). Multi-tiered monitoring enables you to use powerful top-down network monitoring techniques.

Top-down monitoring begins when you notice particular traffic flow patterns in a global view of your network. You then progessively focus in until you find the specific source or sources of the traffic. Using this method, the amount of information you need to assess is kept to a minimum. Top-down monitoring is robust enough to keep you in control of even the most complex and sophisticated networks.

Top-Down Monitoring for the MAC Layer

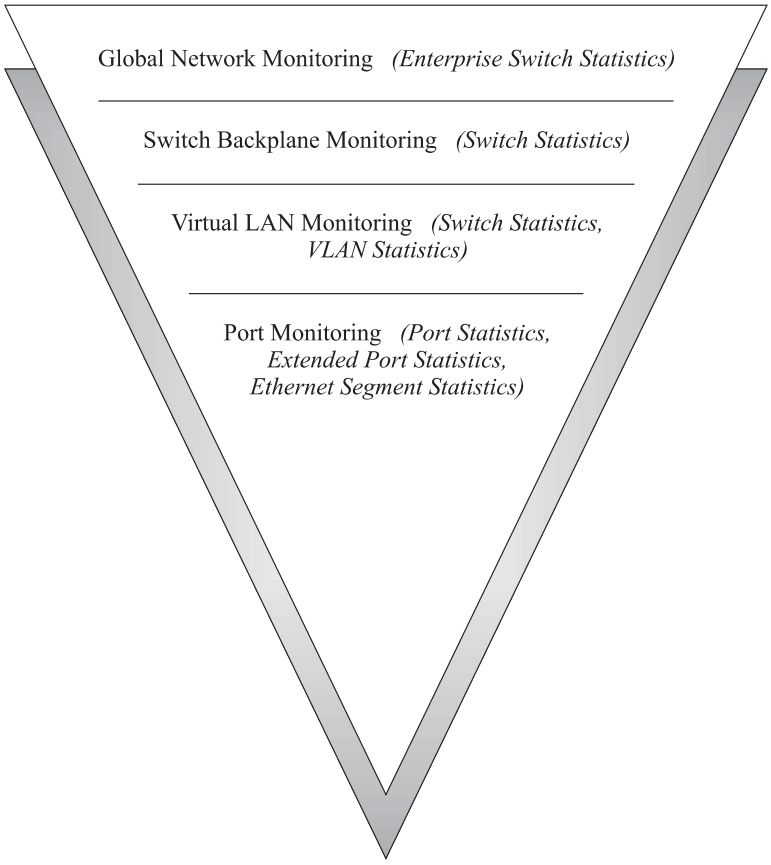
The top tier for Avaya SMON monitoring at the MAC layer (SMON I) is Enterprise Switch Statistics. The Enterprise Switch Statistics tool shows summary traffic statistics for all switches in your network.

The next two tiers provide a general look at the traffic passing through a specific switch. In this way, you can view at a glance whether the switch is functioning efficiently and effectively. These tiers provide answers to questions such as:

- Is there more traffic than usual passing through this switch?
- Are there more error packets than usual?
- How much traffic is passing through the VLANs?
- Do the VLANs have equal loads?

The lower monitoring tiers provide more focused views of the traffic on the device. They allow you to zero in on a specific host or port on a switch. You can then pinpoint the exact source of the traffic discovered in the upper tiers.

Figure 1-2. Top-Down Monitoring for the MAC Layer


Global Network Monitoring (Enterprise Switch Statistics)
Switch Backplane Monitoring (Switch Statistics)
Virtual LAN Monitoring (Switch Statistics, VLAN Statistics)
Port Monitoring (Port Statistics, Extended Port Statistics, Ethernet Segment Statistics)

Top-Down Monitoring for the Upper Layers

Avaya's SMON applications provide a series of AnyLayer SMON tools for implementing top-down monitoring techniques at the network layer and above. Top-down monitoring on upper layers allows you to view aspects of your network that extend beyond the router, or that apply to a specific application protocol.

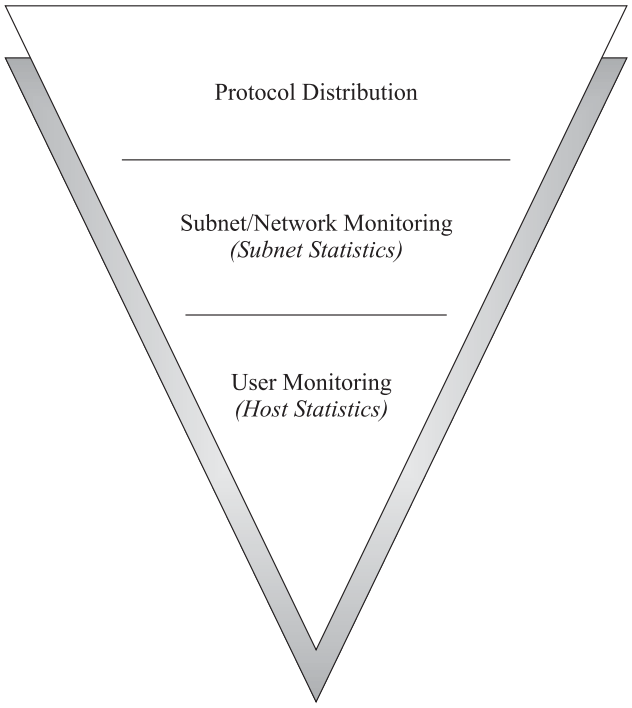
The upper tier of SMON top-down monitoring for upper layers is Protocol Distribution. The Protocol Distribution tool gives a general view of traffic through a switch, organized by protocol. Some of the types of questions Protocol Distribution may provide answers to are:

- What proportion of the traffic consists of IP maintenance protocols, such as ARP, RIP, or SAP?

- Is there an unusual amount of traffic for a specific type of application protocol, such as e-mail, name service, or HTTP?
- Is there an unusual amount of ICMP traffic that may be caused by flood pinging?

The lower tiers then allow you to locate the IP subnet or specific IP host that is the source of the traffic discovered using Protocol Distribution.

Figure 1-3. Top-Down Monitoring for Upper Layers

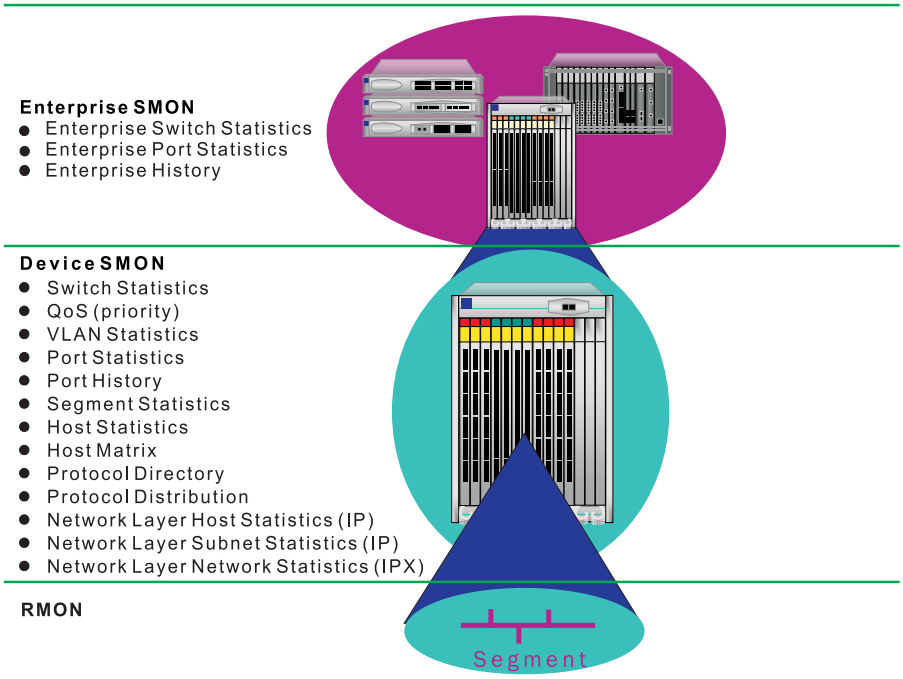


SMON Tools

The SMON tools are divided into the following:

- **Avaya SMON Manager Tools** - These tools provide global monitoring capabilities for multiple SMON devices on a network.
- **Device SMON Tools** - These tools monitor specific devices.

Figure 1-4. SMON Tools



Avaya SMON Manager Tools

Avaya SMON Manager tools provide global monitoring capabilities for multiple SMON devices on a network. There are two types of SMON Manager tools:

- **Online SMON Tools** - Tools providing network-wide switch and port monitoring information in real-time. These tools include:
  - — **Enterprise Switch Statistics**
  - — **Enterprise Port Statistics**
  - — **Enterprise Voice Port Statistics**
- **SMON History Tools** - Tools providing views and reports of monitoring information gathered over time. These tools include:
  - — **Enterprise History**
  - — **Enterprise Switch History**
  - — **Port History**
  - — **Enterprise Voice Port Statistics**

In addition, the Port History tool can be accessed from Enterprise History. These tools enable the network administrator to monitor and control history activities of all switches from two central control screens.

Enterprise Switch Statistics

The Enterprise Switch Statistics tool enables the network administrator to monitor network statistics of all switches on the network level, in a network which supports SMON.

As more and more switches are implemented in networks, it becomes increasingly important to be able to get a quick view of all the switches. The Enterprise Switch Statistics application gives you a bird's-eye view of the switched network, allowing you to see at a glance which switches are functioning properly and which require attention.

All devices on the network which have been discovered by the management umbrella and possess an SMON probe are displayed in a bar.

Enterprise Switch Statistics displays a concise analysis of the traffic traversing the switch. Data is displayed as a bar graph, for an understanding of the exact levels of traffic traversing the switches.

The basic counters (displayed in the bar charts) provide a view of the key counters for each switch. Placing the cursor over each bar displays an Info Box, containing the Type, IP address, and MAC address of the associated device. This allows you to easily track switches.

The Enterprise Switch Statistics view forms the top layer of the MAC level top-down monitoring concept. It allows you to view the level of a specific user to isolate network problems quickly and accurately.

The relevant Device SMON application for each specific device can be opened from within Enterprise Switch Statistics.

Enterprise Port Statistics

Enterprise Port Statistics is an integral part of Avaya SMON Manager. It allows you to see the data passing through selected ports on switches.

For each port, Avaya SMON Manager summarizes the traffic, such as good and error unicasts into the switch, and packets from the switch.

If you notice that a particular port displays a disproportionate number of errors, this may indicate that a specific device connected to the port is responsible. If the attached port supports a Gigabit Ethernet connection, only a few hosts will be attached to this port. This makes it easy to locate the responsible host.

Enterprise Voice Port Statistics

Enterprise Voice Port Statistics allows you to see the information on the data passing through Avaya IP telephones.

For each Avaya IP telephone, Avaya SMON Manager summarizes the traffic, such as good and error unicasts into the switch, and packets from the IP telephone.

If you notice that a particular IP telephone displays a disproportionate number of errors, this may indicate that the specific IP telephone connected to the port may be faulty. In addition, very high traffic statistics for an IP telephone may indicate heavy usage.

Enterprise History

Using the Enterprise History tool, you can easily activate the history mechanism, and upload data from the Avaya M770, Avaya P130, Avaya P330, Avaya C360, Avaya W310, Avaya C460, Avaya P580, and Avaya P882 Device probes.

In addition, you can perform an automatic, periodic upload of data stored in the probes during the collection period and store this data for later analysis.

For the Enterprise History application, the agent stores up to 360 separate data samples at equal time intervals that can later be retrieved from the SMON console. This is called History data, and provides an alternative method for analyzing the data in a switched network. The agent collects port history counters for all the ports in a device.

The Enterprise History application is a control center for managing the collection of History data on all agents in the network. Its main tasks are:

- Showing the status of Port History on each agent.
- Enabling the uploading of History data stored on each of the agents.
- Activating Port History on the console to display the History data stored on an agent.

The main advantages of using History data are:

- Quality information about network performance are received. After analyzing the performance, you can plan accordingly for expected times when ports on the network are reaching their full capacity.
- Data is collected on all switch ports at the same time.
- Statistics can be imported into an external application, such as a database or spreadsheet, for more detailed analysis.
- Data can be graphically displayed to view history behavior.

The Enterprise History application can save History data from the agents in the network manually or automatically. Manual upload means that you must select an agent and then activate the upload. Automatic upload means that the Enterprise History application saves the data according to a predefined interval for selected agents.

Enterprise Switch History

Enterprise Switch History provides the option to use two collections at the same time, a long term collection and a short term collection. The short term collection consists of data collected at brief intervals. This provides a complete breakdown of network performance over a few hours or days. The long term collection consists of data collected at longer intervals over a period of a few days or weeks. This method provides a long term view of the network.

A collection period is divided into a maximum number of separate samples. You can upload the data at any time during the collection period, even before it is completed. By analyzing this data using Port History, you can view the times and locations of the peak activity periods on the network.

The key parameters for collections are:

- **Collection Duration** - The interval for each collection. This defines how long the agent collects and stores the History data. For example, a collection duration of 2 weeks, results in the agent collecting and storing data for 2 weeks. The longer the collection, the longer the interval between when the agent collects data.
- **Status** - This defines whether a collection is active (the agent collects data) or inactive (the agent does not collect data). When setting an automatic upload of data for a Collection, the management station only uploads data for active Collections.

Port History

Using the Port History tool, you can access detailed history information collected by an SMON probe. This application is launched from the Enterprise Switch History application.

The benefits of Port History include:

- Quality information reports about the performance of specific ports.
- The ability to work on all switch ports at the same time.
- The ability to plan for expected times when ports on the network are reaching their full capacity after analyzing the performance.
- The ability to view the effect of a change of configuration on the performance of the network. You can also view the exact details of the change itself in terms of which modules were inserted or removed.
- The ability to discover the time a reported problem occurred and on which port.
- The ability to view the ports and times where the traffic is at its highest or lowest.
- The ability to import the statistics into an external application, such as a database or spreadsheet, for more detailed analysis.
- The ability to view individual port history statistics in graph form.

Device SMON Tools

Device SMON tools monitor specific devices and provide statistics on the traffic passing through a device's switch fabric, a VLAN, port, and host. In addition, Device SMON can provide information about host pairs talking to each other.

For information on Device SMON tools, refer to the appropriate *Avaya Device SMON User Guide*.

2 Introduction to Avaya SMON Manager

This chapter provides an introduction to Avaya SMON Manager, and contains the following sections:

- **Starting Avaya SMON Manager** - Instructions on starting Avaya SMON Manager.
- **The Online SMON User Interface** - A detailed description of the Online SMON user interface.
- **Working with SMON Tools** - Techniques for using Online SMON more effectively.

Starting Avaya SMON Manager

To start Avaya SMON Manager from Avaya Network Management Console, select **Tools** > **Avaya SMON Manager**. Avaya SMON Manager opens with the Online SMON window.

To start Avaya SMON Manager from HP-OV NNM (UNIX or NT-OV), select **Tools** > **Avaya** > **Avaya SMON Manager**. Avaya SMON Manager opens with the Online SMON window.

The Online SMON User Interface

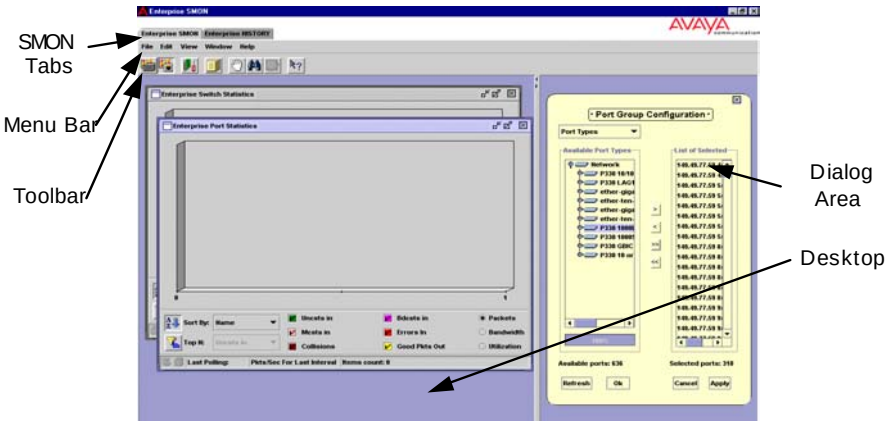
The user interface consists of the following elements:

- **SMON Tabs** - Tabs providing a method for switching between Online SMON and SMON History.
- **Menu Bar** - Menus for accessing Online SMON functions. For information on the full menu structure in Online SMON, refer to "Online SMON Menus" on page 77.
- **Online SMON Toolbar** - Buttons providing shortcuts to important functions in Online SMON.
- **Desktop** - A resizeable window where Online SMON windows are displayed.

- **Dialog Area** - A resizeable window where all dialog boxes appear.

The figure below shows the user interface, with its various parts labeled.

Figure 2-1. Online SMON User Interface



SMON Tabs

The SMON tabs provide a method for switching between the Online SMON window and the SMON History window. To view a window, click the appropriate SMON tab. The relevant window appears.

Online SMON Toolbar

The Toolbar provides shortcuts to the main Online SMON functions and tools. The following table describes the buttons on the toolbar and lists the equivalent menu options.

Table 2-1. Online SMON Toolbar Buttons

Button	Description	Menu
	Activates the Switch Statistics tool.	**File > New > Switch Statistics**
	Activates the Port Statistics tool.	**File > New > Port Statistics**
	Activates the Voice Port Statistics tool.	**File > New > Voice Port Statistics**
	Opens the Configuration dialog box.	**Edit > Configuration**

Table 2-1. Online SMON Toolbar Buttons (Continued)

Button	Description	Menu
	Produces a report file for importing to a spreadsheet or word processor.	**File > Report Now**
	Temporarily stops and then restarts collection of SMON data. When the collection of SMON data is paused, the background of the chart appears white.	**View > Pause**
	Searches for a specific item.	**Edit > Find**
	Opens the Customize View dialog box.	**View > Customize**
	Opens context sensitive on-line help.	**Help > Help On**

If a tool is not active, clicking the corresponding Online SMON toolbar button launches the tool. If a tool is already active, clicking the corresponding Online SMON toolbar button brings the tool to the foreground. For more information about the individual tools, refer to "Avaya SMON Manager Tools" on page 10.

Dialog Area

The area on the right side of the user interface is where all dialog boxes appear. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens it replaces the current dialog box in the Dialog Area.

Desktop

The left side of the application window is the Desktop. This area can be resized by dragging the vertical splitter bar with the mouse. Online SMON windows can be resized and minimized. Minimized windows are shown at the bottom of the Desktop.

Working with SMON Tools

The following sections describe features that can help you use Online SMON tools more effectively. The topics include:

- **Configuring Display Options** - Instructions on how to configure general Online SMON options.
- **Configuring Report Options** - Instructions on how to configure display options in the Switch, Port, and Voice Port Statistics applications.
- **Using Dialog Box Options** - Instructions on using the dialog box options.
- **Generating Reports** - Instructions on how to generate reports.
- **Managing Windows** - Instructions on how to manage Online SMON windows.

Configuring Display Options

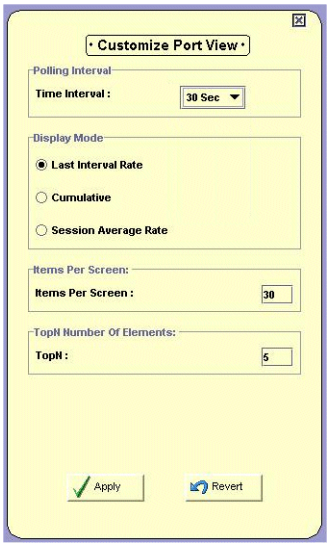
To configure display options for Enterprise Switch, Port, or Voice Port Statistics:

1. Activate the application for which you want to configure display options.
2. Click .

   Or

   Select **View** > **Customize**. The Customize View dialog box opens.

Figure 2-2. Customize View Dialog Box



The Customize View dialog box enables you to change the following options:

- **Polling Interval**
- **Display Mode**
- **Items Per Screen**
- **TopN Number of Elements**

Polling Interval

The Polling Interval option allows you to configure the way in which information is collected. If you make the polling interval smaller, you receive more accurate data at the expense of using more network resources. The objective is to use the ideal polling interval that provides accurate data using minimum network resources.

To change the polling interval, select a polling interval from the Polling Interval pull-down listbox.

The following polling intervals can be selected:

- 30 seconds
- 1 minute
- 5 minutes
- 15 minutes
- 30 minutes
- 60 minutes

*** Note:** The new polling interval will take effect when the device is next polled.

Display Mode

The Display Mode option allows you to select one of three display modes. Select a display mode using the option buttons.

The display mode options are:

- Last Interval Rate - The statistics gathered since the last poll.
- Cumulative - The accumulated statistics gathered since the start of the session.
- Session Average Rate - The average of the statistics per polling interval since the start of the session.

Items Per Screen

The Items Per Screen enables you to configure the number of switches, ports, and LAGs visible in the Enterprise Switch or Port Statistics windows. To change the number of items visible on the screen, enter a number in the Items Per Screen field.

*** Note:** The number of items per screen must be between 1 and 15.

TopN Number of Elements

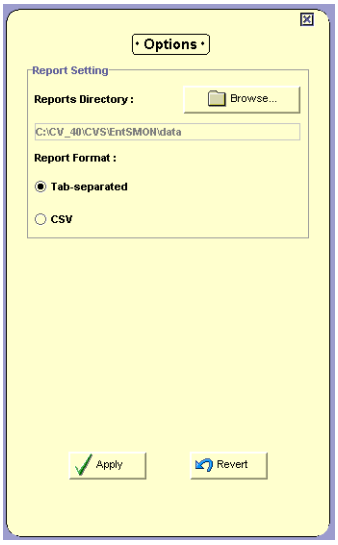
The TopN Number of Elements option enables you to configure the number of switches, ports, and LAGs visible in the Enterprise Switch or Port Statistics windows, using TopN filtering. TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

To configure the TopN number of elements, enter the number of items to display in the Enterprise Switch or Port Statistics window in the TopN field.

Configuring Report Options

To configure report options for Enterprise Switch, Port, and Voice Port Statistics, select **File** > **Options**. The Options dialog box opens.

Figure 2-3. Options Dialog Box



The Options dialog box enables you to select a default directory for saving reports and configure the report format.

To select a default directory for saving reports:

1. Click **Browse**. A directory browser window opens.
2. Navigate to the directory in which you want to save reports.
3. Click **Open**. The path appears in the Reports Directory field.

To select a report format, select one of the following options:

- Tab-separated - The report is formatted as a tab-delimited file.
- CSV - The report is formatted as a comma-delimited file.

For more information on reports, refer to "Generating Reports" on page 22.

Using Dialog Box Options

Information entered in a dialog box is not saved until you click the **Apply** button.

To undo all changes made to the information in the dialog box, click **Revert**. The information in the dialog box reverts to what it was when the dialog box was first opened.

If you have already sent information to the device from the dialog box and you click **Revert**, the information in the dialog box reverts to what it was when it was last applied.

*** Note:** When clicking **Revert**, the application does not poll the device for information. It is therefore possible that the dialog box may not reflect the true state of the device.

Generating Reports

You can produce two types of reports with Enterprise SMON Manager:

- **Report Now**
- **Auto Report**

Generated reports are text files that can be imported into spreadsheets such as Excel and database programs such as Access. The reports can be generated in a tab delimited format or a comma separated format. When a report is generated, it is saved to the directory specified in the Reports Directory field in the General Options dialog box.

Data in a Report Now includes only the statistics collected during the last polling interval. In an Auto Report, statistics collected at each polling interval are appended to the report.

For more information on selecting a format and a default directory for reports, refer to "Configuring Report Options" on page 21.

Report Now

To generate a report with the statistics from the last time the device was polled:

1. Click .

   Or

   Select **File** > **Report Now**. The Report Now dialog box opens.

Figure 2-4. Report Now Dialog Box

2. To change the filename and directory in which to save the report:

   a. Click **Browse**. A file browser window opens.

   b. Select a directory and filename for the report.

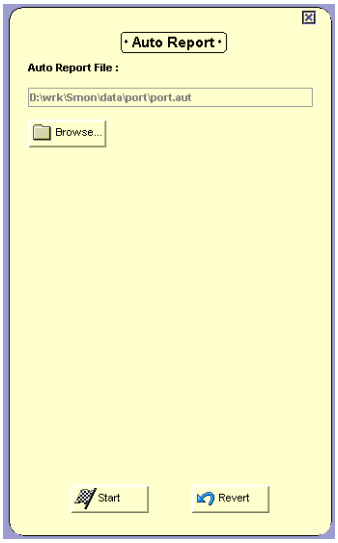
3. Click **Report**. The report is generated.

Auto Report

To start generating an automatic report:

1. Select **File** > **Auto Report**. The Auto Report dialog box opens.

Figure 2-5. Auto Report Dialog Box



2. To change the filename and directory in which to save the reports:
   a. Click **Browse**. A file browser window opens.
   b. Select a directory and filename for the report.
3. Click **Start**. The report is generated immediately. Data is added to the report after each polling interval.

CAUTION

Auto Reports are automatically saved to the network management station (NMS). If Auto Reports are generated on many devices for a long period of time, and none of the files are deleted, the NMS's hard disk may become full.

If this occurs, stop the applications that are generating automatic reports and delete the files that are not required.

To stop generating Auto Reports:

1. Select **File** > **Auto Report**. The Auto Report dialog box opens.
2. Click **Stop**.

Or

1. Close Avaya SMON Manager. Auto Reports are no longer generated.

Managing Windows

Online SMON enables you to manage open windows easily.

To cascade all open windows, select **Window > Cascade**.

To bring the next window in the list to the front, select **Window > Next**.

To bring the previous window in the list to the front, select **Window > Previous**.

To close all windows, select **Window > Close All**.

To bring a window in the list to the front, select **Window >** *Window Name*, where *Window Name* is the name of the window you want to view.

3 Switch Statistics

Switch Statistics allows you to see the data passing through each switch in the network. For a detailed overview of Enterprise Switch Statistics, refer to "Enterprise Switch Statistics" on page 10.

Accessing Switch Statistics

To access the Switch Statistics window:

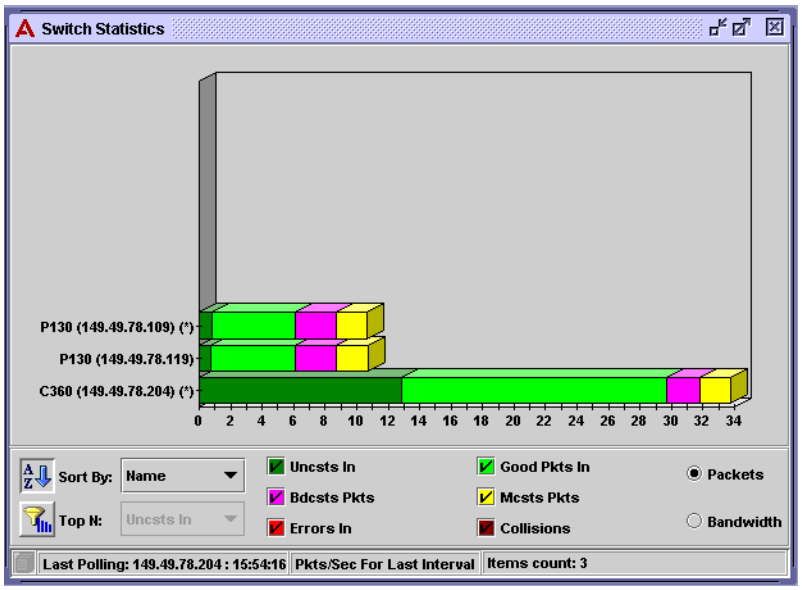
1. Click .

   Or

   Select **File > New > Switch Statistics**. The Switch Statistics application opens with the Switch Group Configuration dialog box open.

2. Select the switches you want SMON to poll. For instructions on selecting switches for polling, refer to "Selecting Switches to Poll" on page 30. The Switch Statistics window displays the selected switches and their traffic.

Figure 3-1. Switch Statistics Window



Using Switch Statistics

The Switch Statistics window allows you to see the data passing through each switch in the network. For an explanation of the Switch Statistics window, refer to "Understanding the Switch Statistics Window" on page 28.

Using Switch Statistics you can:

- Select the switches you want SMON to monitor. For information on selecting switches to monitor, refer to "Selecting Switches to Poll" on page 30.
- Select the switches you want SMON to display. For information on changing display options, refer to "Filtering the Switch Statistics Display" on page 32.
- Select the counters you want SMON to display. For information on selecting counters, refer to "Switch Statistics Counters" on page 32.
- Sort the display. For more information on sorting the display, refer to "Sorting the Display" on page 33.
- Search for specific devices. For more information, refer to "Searching for Switches" on page 34.

Understanding the Switch Statistics Window

The Switch Statistics window is organized as follows:

- The X axis represents packets.
- The Y axis represents switches. Each row on the graph corresponding to a switch is labeled on the Y axis with the IP address of the switch or the user defined name for the switch.
- The following indicators can appear after the device name:
  - **[NS]** - The device is not supported by SMON.
  - **[DP]** - The device has a duplicated SMON license.
  - **[NR]** - The device is currently not responding.
  - **[NL]** - The device has no SMON license.
  - **[SG]** - The device information includes segment traffic.

— **(*)** - Extra information about the port is available in the port's Info Box.

— **(**)** - There are errors on the device. View the device's Info Box for more detailed information.

- The table below describes the items found in the Switch Statistics status bar.

Table 3-1. Switch Statistics Status Bar Items

Item	Description
Last Polling	The IP address of the last device polled and the time when the device was last polled.
Pkts/Sec For Last Interval	The average bandwidth utilization for the device over the last polling interval.
Items count	Total number of devices being polled.

Switches in the Switch Statistics window can be labeled with the switch's IP address (the default device name) or the user defined name for the switch. To toggle the display of user defined names for switches, select **View > Switch Default Naming**. The display of user defined names for switches is toggled.

For information on Switch Statistics counters, refer to "Switch Statistics Counters" on page 32.

For more information about modifying the display, and the available toolbar, status bar, and mouse movement options, refer to "Configuring Display Options" on page 19.

Selecting Switches to Poll

To reduce strain on the network, Avaya SMON Manager enables you to select the switches that are monitored. SMON only polls the switches you select. Select the switches you want SMON to monitor using the Switch Group Configuration dialog box.

In addition, using the Switch Group Configuration dialog box you can save groups of switches to be monitored.

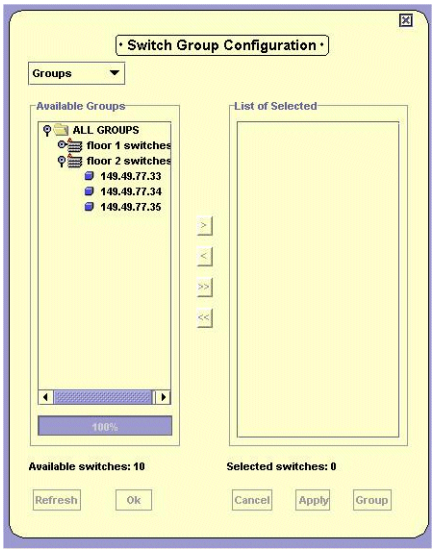
To open the Switch Group Configuration dialog box:

Click .

Or

Select **Edit** > **Configuration**. The Switch Group Configuration dialog box opens.

Figure 3-2. Switch Group Configuration Dialog Box



The Known Network box shows the devices in the network. You can monitor the progress of the learning process in the progress bar, located below the Known Network box.

To sort the switches displayed in the Known Network listbox, select a sorting method from the pull-down list above the Known Network listbox. Sorting methods include:

- **IP Address** - The devices are sorted by IP address.
- **Device Type** - The devices are sorted by device type.

- **Groups** - The devices are sorted by groups. Only devices in groups are listed. Moving a group to the List of Selected, selects all devices that are members of the group.

To refresh the Known Network list, click **Refresh**. The devices in the network are relearned.

*** Note:** Clicking **Refresh** also refreshes the list of device ports in the Port Group Configuration dialog box and the list of IP telephones in the Voice Port Configuration dialog box.

To add switches to the List of Selected:

Select switches from the Known Network and click >.

Or

Double-click switches in the Known Network. The selected switches appear in the List of Selected.

To select all switches, click >>. All switches are added to the List of Selected.

To remove switches from the List of Selected:

Select the switches in the List of Selected and click <.

Or

Double-click switches in the List of Selected. The selected switches are removed from the List of Selected.

To remove all items from the List of Selected, click <<. All switches are removed from the List of Selected.

To save the switches in the List of Selected as a group:

1. Click **Group**. The Save Group dialog box opens.

Figure 3-3. Save Group Dialog Box

2. Enter a name for the group.
3. Click **OK**. The switch group is created.

Filtering the Switch Statistics Display

By default, information from all switches selected in the Switch Group Configuration dialog box is displayed in the Switch Statistics window. You can limit information being displayed to specific ports using TopN filtering. This makes it easier to concentrate on specific devices in the network.

TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON selects the TopN items by a rate base which you select from the pull-down listbox in the Switch Statistics window. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

For information on defining the number of items to display using TopN filtering, refer to "TopN Number of Elements" on page 20.

To activate the TopN filter, click at the bottom of the Enterprise Switch Statistics window. To deactivate the TopN filter, click at the bottom of the Enterprise Switch Statistics window.

To select a rate base, select a TopN criteria from the TopN pull-down listbox at the bottom of the Enterprise Switch Statistics window.

Switch Statistics Counters

To select a set of statistics to display, click one of the option buttons on the lower right-hand corner of the window. The statistics sets are:

- **Packets** - Counters for selected packet types for each switch.
- **Bandwidth** - The rate at which traffic is entering and exiting each switch.

The counters relevant to the selected set of statistics appear under the graph. Check the counters you want displayed. Statistics for the checked counters are displayed as bar graphs.

The following table lists the Switch Statistics counters in the Packets statistics set.

Table 3-2. Switch Statistics Counters - Packets

Counter	Description
Uncsts In	The number of good unicast packets entering the switch.
Good Pkts In	The number of good packets entering the switch.
Bdcsts Pkts	The number of good broadcast packets entering the switch.
Mcsts Pkts	The number of good multicast packets entering the switch.
Errors In	The number of error packets filtered out by the switch.
Collisions	The number of collisions occurring on the switch.

The following table lists the Switch Statistics counter in the Bandwidth statistics set.

Table 3-3. Switch Statistics Counter - Bandwidth

Counter	Description
In BW	The rate at which traffic is entering the switch in Kbps.

Sorting the Display

You can sort the display by the device name or any of the counters available for the device.

To sort the display:

1. Click . The display is sorted by the selected criteria.
2. Select a sorting criterion from the Sort By pull-down listbox.

When sorting by Name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

Searching for Switches

The Find option allows you to locate a specific switch in the Switch Statistics window.

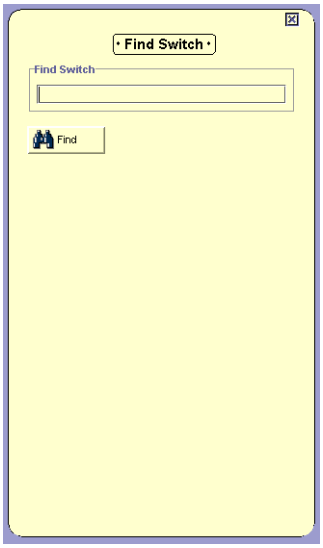
To search for a switch:

1. Click .

   Or

   Select **Edit** > **Find**. The Find Switch dialog box opens.

Figure 3-4. Find Switch Dialog Box



2. Enter the switch name or IP address in the Find Switch field.
3. Click **Find**. The found device is highlighted for easy identification.

*** Note:** If you enter only part of the name or IP address, SMON will find the first time the value appears.

To remove the highlight from the application window, click in the Switch Statistics window. The highlight disappears.

*** Note:** The Find button changes to Find Next until all instances of the search information have been found.

4 Port Statistics

Port Statistics allows you to see the data passing through each port and LAG in the network. For a detailed overview of Enterprise Port Statistics, refer to "Enterprise Port Statistics" on page 11.

Accessing Port Statistics

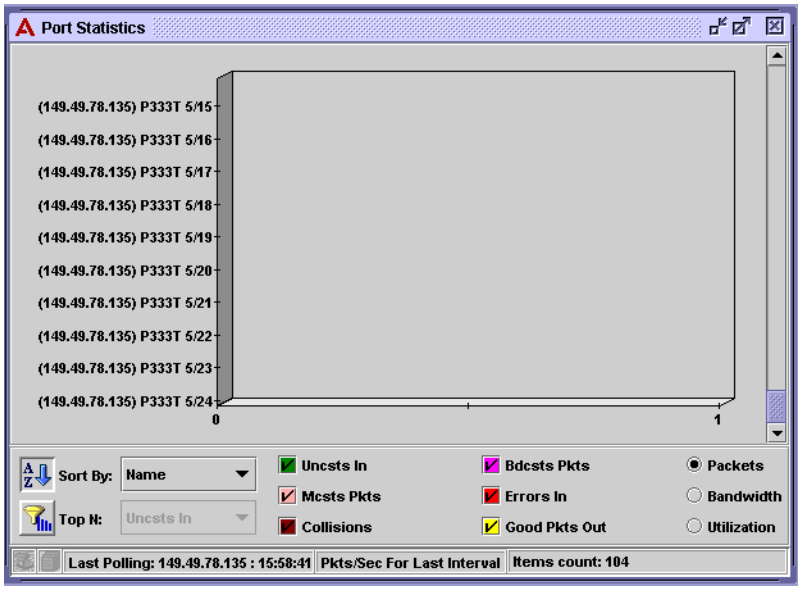
To access the Port Statistics window:

Click .

Or

Select **File > New > Port Statistics**. The Port Statistics application opens with the Port Group Configuration dialog box open.

Figure 4-1. Port Statistics Window



Using Port Statistics

The Port Statistics window allows you to see the data passing through each port in the network. For an explanation of the Port Statistics window, refer to "Understanding the Port Statistics Window" on page 36.

Using Port Statistics you can:

- Select the ports and LAGs you want SMON to monitor. For information on selecting ports and LAGs to monitor, refer to "Selecting Ports and LAGs to Poll" on page 38.
- Select the ports and LAGs you want SMON to display. For information on changing display options, refer to "Filtering the Port Statistics Display" on page 40.
- Select the counters you want SMON to display. For information on selecting counters, refer to "Port Statistics Counters" on page 43.
- Sort the display. For more information on sorting the display, refer to "Sorting the Display" on page 44.
- Search for specific ports and LAGs. For more information, refer to "Searching for Ports and LAGs" on page 45.

Understanding the Port Statistics Window

The Port Statistics window is organized as follows:

- The X axis represents packets or percentage of utilization.
- The Y axis represents ports and LAGs. Each row on the graph corresponding to a port or LAG is labeled on the Y axis with a port number, LAG number, or with the user defined name of a port.
- An asterisk **(*)** following the name of a port or LAG indicates that extra information about the port is available in the port's Info Box.

- The table below describes the items found in the Port Statistics status bar.

Table 4-1. Port Statistics Status Bar Items

Item	Description
Last Polling	The IP address of the last device polled and the time when the device was last polled.
Pkts/Sec For Last Interval	The average bandwidth use over the last polling interval.
Items count	Total number of ports being polled.

Ports in the Port Statistics window can be labeled with the port's IP address and port number (the default device name) or the user defined name for the port. LAGs in the Port Statistics window can be labeled with the LAG's IP address and LAG number (the default device name) or the user defined name for the LAG. To toggle the display of user defined names for ports and LAGs, select **View > Port Default Naming**. The display of user defined names for ports and LAGs is toggled.

*** Note:** For high-speed ports and LAGs with large polling intervals, bandwidth and utilization counters may be inaccurate.

For information on Port Statistic counters, refer to "Port Statistics Counters" on page 43.

For more information about modifying the display, refer to "Configuring Display Options" on page 19.

Selecting Ports and LAGs to Poll

To reduce strain on the network, Avaya SMON Manager enables you to select the ports and LAGs that are monitored. SMON only polls the ports and LAGs you select. Select the ports and LAGs you want SMON to monitor using the Port Group Configuration dialog box.

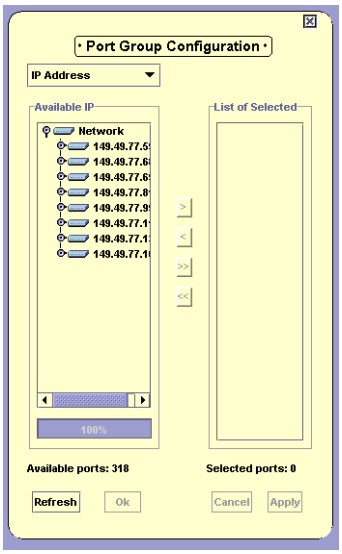
To open the Port Group Configuration dialog box:

Click .

Or

Select **Edit > Configuration**. The Port Group Configuration dialog box opens.

Figure 4-2. Port Group Configuration Dialog Box



The Known Ports box shows the device ports in the network. You can monitor the progress of the learning process in the progress bar, located below the Known Ports box.

To sort the ports displayed in the Known Ports listbox, select a sorting method from the pull-down list under the Known Ports listbox. Sorting methods include:

- **IP Address** - The ports are sorted by IP address.
- **Valuable Ports** - Only valuable ports appear in the Known Ports listbox.
- **Port Type** - The ports are sorted by port type.

- **VLAN** - The ports are sorted and represented by VLAN. When using the **VLAN** sorting method a list of VLANs appears in the Known Ports list. Moving a VLAN to the List of Selected, selects all ports that are members of the VLAN.
- **Groups** - The ports are sorted by groups. Only ports in groups are listed. Moving a group to the List of Selected, selects all ports that are members of the group.

*** Note:** Selecting **Network**, a device, module, port type, or VLAN, selects all ports under the selected object.

To refresh the Known Ports list, click **Refresh**.

*** Note:** Clicking **Refresh** also refreshes the list of switches in the Switch Configuration dialog box and the list of IP telephones in the Voice Port Configuration dialog box.

To add ports and LAGs to the List of Selected:

Select ports and LAGs from the Known Ports and click >.

Or

Double-click ports and LAGs in the Known Ports. The selected ports and LAGs appear in the List of Selected.

To select all ports and LAGs, click >>. All ports and LAGs are added to the List of Selected.

To remove ports and LAGs from the List of Selected:

Select the ports and LAGs in the List of Selected and click <.

Or

Double-click ports and LAGs in the List of Selected. The selected ports and LAGs are removed from the List of Selected.

To remove all items from the List of Selected, click <<. All ports and LAGs are removed from the List of Selected.

To save the ports and LAGs in the List of Selected as a group:

1. Click **Group**. The Save Group dialog box opens.

Figure 4-3. Save Group Dialog Box

2. Enter a name for the group.
3. Click **OK**. The port group is created.

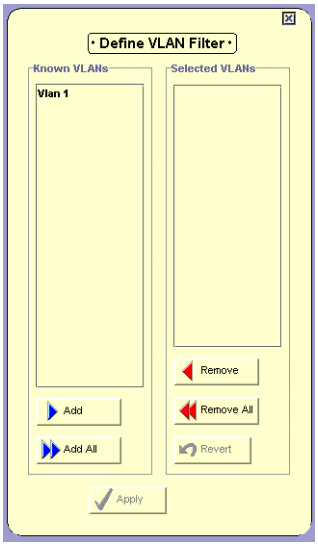
Filtering the Port Statistics Display

By default, information from all ports and LAGs selected in the Port Group Configuration dialog box is displayed in the Port Statistics window. You can limit information being displayed to specific ports and LAGs using VLAN and TopN filters. In addition, you can sort the display. For information on sorting the display, refer to "Sorting the Display" on page 44.

VLAN Filtering

You can filter the ports and LAGs displayed in the Port Statistics window by VLAN. Only ports that are members of the selected VLANs are displayed in the Port Statistics window. This makes it easier to concentrate on specific VLANs in the network. To open the VLAN Filter dialog box, select **View > Define VLAN Filter**. The VLAN Filter dialog box opens.

Figure 4-4. VLAN Filter Dialog Box



To add VLANs to the Selected VLANs list:

Select VLANs from the Known VLANs list and click **Add**.

Or

Double-click VLANs in the Known VLANs list. The selected VLANs appear in the Selected VLANs list.

To select all VLANs, click **Add All**. All VLANs are added to the Selected VLANs list.

To remove VLANs from the Selected VLANs list:

Select VLANs in the Selected VLANs list and click **Remove**.

Or

Double-click VLANs in the Selected VLANs list. The selected VLANs are removed from the Selected VLANs list.

To remove all items from the Selected VLANs list, click **Remove All**. All VLANs are removed from the Selected VLANs list.

To apply the VLAN filter, click **Apply**. The Port Statistics information is filtered.

To toggle the VLAN filter, select **Actions** > **Activate VLAN Filter**.

TopN Filtering

TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON selects the TopN items by a rate base which you select from the pull-down listbox in the Port Statistics window. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

For information on defining the number of items to display using TopN filtering, refer to "TopN Number of Elements" on page 20.

To activate the TopN filter, click at the bottom of the Enterprise Port Statistics window. To deactivate the TopN filter, click at the bottom of the Enterprise Port Statistics window.

To select a rate base, select a TopN criteria from the TopN pull-down listbox at the bottom of the Enterprise Port Statistics window.

Port Statistics Counters

To select a set of statistics to display, click one of the option buttons on the lower right-hand corner of the window. The statistics sets are:

- **Packets** - Counters for selected packet types for each port.
- **Bandwidth** - The rate at which traffic is entering and exiting each port.
- **Utilization** - The utilized capacity of each port.

The counters relevant to the selected set of statistics appear under the graph. Check the counters you want displayed. Statistics for the checked counters are displayed as bar graphs.

The following table lists the Port Statistics counters in the Packets statistics set.

Table 4-2. Port Statistics Counters - Packets

Counter	Description
Uncsts In	The number of good unicast packets entering the switch.
Bdcsts Pkts	The number of good broadcast packets entering the switch.
Mcsts Pkts	The number of good multicast packets entering the switch.
Errors In	The number of error packets filtered out by the switch.
Collisions	The number of collisions occurring on the port or LAG.
Good Pkts Out	The number of good packets leaving the switch.

The following table lists the Port Statistics counters in the Bandwidth statistics set.

Table 4-3. Port Statistics Counters - BandWidth

Counter	Description
In BW	The rate at which traffic is entering the port or LAG in Kbps.
Out BW	The rate at which traffic is exiting the port or LAG in Kbps.

The following table lists the Port Statistics counters in the Utilization statistics set.

Table 4-4. Port Statistics Counters - Utilization

Counter	Description
Util	The average percentage of the port's capacity utilized in the last polling interval.

Sorting the Display

You can sort the display by the device name or any of the counters available for the device.

To sort the display:

1. Click . The display is sorted by the selected criteria.
2. Select a sorting criterion from the Sort By pull-down listbox.

When sorting by Name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

Searching for Ports and LAGs

The Find option allows you to locate a specific port in the Port Statistics window.

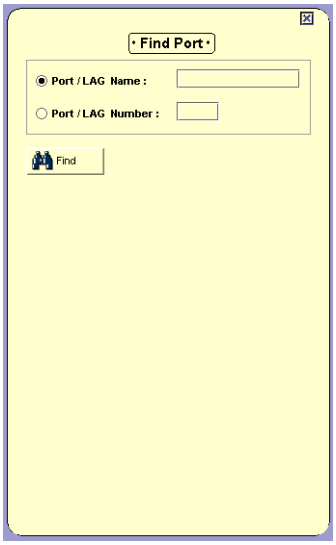
To search for a port or LAG:

1. Click .

   Or

   Select **Edit** > **Find**. The Find Port dialog box opens.

Figure 4-5. Find Port Dialog Box



2. Do one of the following:

- To search for a port or LAG by name:

   a. Click the Port/LAG Name option button.

   b. Enter the port name or part of the port name in the Port/LAG Name field.

   c. Click **Find**. The found port or LAG is highlighted for easy identification.

*** Note:** If you enter only part of the name, SMON will find the first time the value appears.

- To search for a port or LAG by port number:

  a. Click the Port/LAG Number option button.

  b. Enter the port number in the Port/LAG Number field.

  c. Click **Find**. The found port or LAG is highlighted for easy identification.

To remove the highlight from the application window, click in the Port Statistics window. The highlight disappears.

*** Note:** The Find button changes to Find Next until all instances of the search information have been found.

5 Voice Port Statistics

Voice Port Statistics allows you to see the data passing through each Avaya IP telephone in the network. For a detailed overview of Enterprise Voice Port Statistics, refer to "Enterprise Voice Port Statistics" on page 11.

Accessing Voice Port Statistics

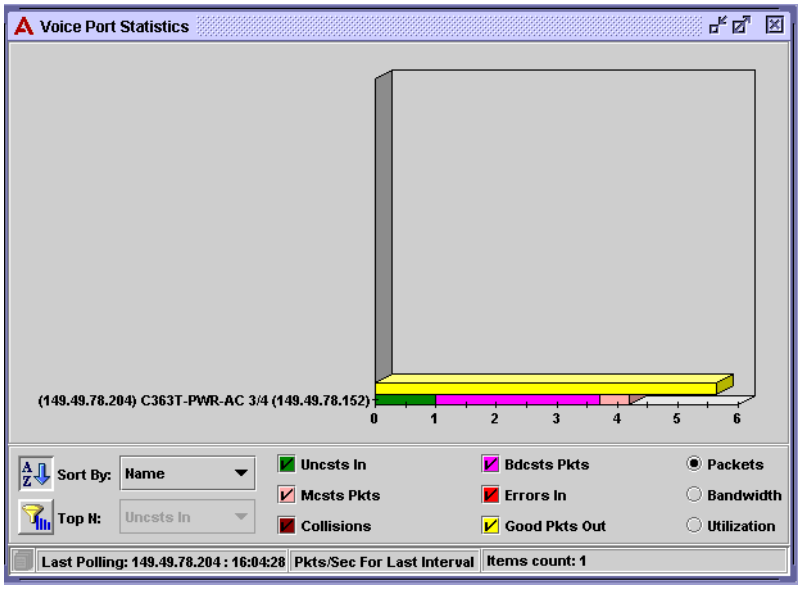
To access the Voice Port Statistics window:

Click .

Or

Select **File > New > Voice Port Statistics**. The Voice Port Statistics application opens with the Voice Port Group Configuration dialog box open.

Figure 5-1. Voice Port Statistics Window



Using Voice Port Statistics

The Voice Port Statistics window allows you to see the data passing through each Avaya IP telephone in the network. For an explanation of the Voice Port Statistics window, refer to "Understanding the Voice Port Statistics Window" on page 48.

Using Voice Port Statistics you can:

- Select the IP telephones you want SMON to monitor. For information on selecting IP telephones to monitor, refer to "Selecting IP Telephones to Poll" on page 50.
- Select the IP telephones you want SMON to display. For information on changing display options, refer to "Filtering the Voice Port Statistics Display" on page 52.
- Select the counters you want SMON to display. For information on selecting counters, refer to "Voice Port Statistics Counters" on page 53.
- Sort the display. For more information on sorting the display, refer to "Sorting the Display" on page 54.
- Search for specific IP telephones. For more information, refer to "Searching for IP Telephones" on page 55.

Understanding the Voice Port Statistics Window

The Voice Port Statistics window is organized as follows:

- The X axis represents packets or percentage of utilization.
- The Y axis represents IP telephones. Each row on the graph corresponding to an IP telephone is labeled on the Y axis with the IP address of the IP telephone.
- An exclamation point (**!**) following the name of an IP telephone indicates that it is a one-cable configuration. This means that a host is connected to the switch through the repeater mounted on the IP telephone. Traffic generated by the host is reported as part of the IP telephone's traffic.

- The table below describes the items found in the Voice Port Statistics status bar.

Table 5-1. Voice Port Statistics Status Bar Items

Item	Description
Last Polling	The IP address of the last IP phone being polled and the time when the IP phone was last polled.
Pkts/Sec For Last Interval	Average bandwidth utilization over the last polling interval.
Items count	Total number of IP telephones being polled.

For more information on Voice Port Statistics counters, refer to "Voice Port Statistics Counters" on page 53.

For more information about modifying the display, refer to "Configuring Display Options" on page 19.

Selecting IP Telephones to Poll

To reduce strain on the network, Avaya SMON Manager enables you to select the IP telephones that are monitored. SMON only polls the IP telephones you select. Select the IP telephones you want SMON to monitor using the Voice Port Group Configuration dialog box.

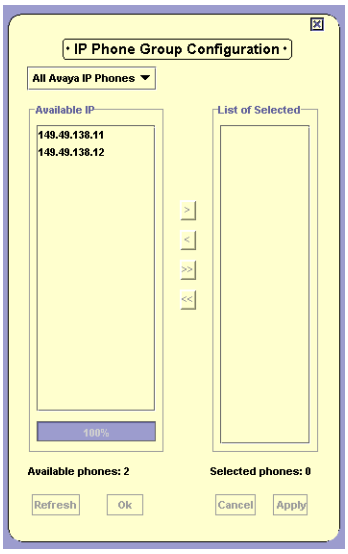
To open the Voice Port Group Configuration dialog box:

Click .

Or

Select **Actions** > **Configuration**. The Voice Port Group Configuration dialog box opens.

Figure 5-2. Voice Port Group Configuration Dialog Box



The Known IP Phones box shows the IP telephones in the network. You can monitor the progress of the learning process in the progress bar, located below the Known IP Phones box.

To sort the IP telephones displayed in the Known IP Phones listbox, select a sorting method from the pull-down list under the Known IP Phones listbox. Sorting methods include:

- **IP Address** - The IP telephones are sorted by IP address.
- **IP Phone Type** - The IP telephones are sorted by IP telephone type.

*** Note:** Selecting **Network** or IP telephone type, selects all IP telephones under the selected object.

To refresh the Known IP Phones list, click **Refresh**.

*** Note:** Clicking **Refresh** also refreshes the list of switches in the Switch Configuration dialog box and the list of ports in the Port Configuration dialog box.

To add IP telephones to the List of Selected:

Select IP telephones from the Known Network and click >.

Or

Double-click IP telephones in the Known Network. The selected IP telephones appear in the List of Selected.

To select all IP telephones , click >>. All IP telephones are added to the List of Selected.

*** Note:** If the application cannot determine the port to which the IP telephone is directly linked, the IP telephone cannot be moved to the List of Selected.

To remove IP telephones from the List of Selected:

Select the IP telephones in the List of Selected and click <.

Or

Double-click IP telephones in the List of Selected. The selected IP telephones are removed from the List of Selected.

To remove all IP telephones from the List of Selected, click <<. All IP telephones are removed from the List of Selected.

Filtering the Voice Port Statistics Display

By default, information from all IP telephones selected in the Voice Port Group Configuration dialog box is displayed in the Voice Port Statistics window. You can limit information being displayed to specific IP telephones using TopN filtering. This makes it easier to concentrate on specific devices in the network.

TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON selects the TopN items by a rate base which you select from the pull-down listbox in the Switch Statistics window. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

For information on defining the number of items to display using TopN filtering, refer to "TopN Number of Elements" on page 20.

To activate the TopN filter, click at the bottom of the Enterprise Voice Port Statistics window. To deactivate the TopN filter, click at the bottom of the Enterprise Voice Port Statistics window.

To select a rate base, select a TopN criteria from the TopN pull-down listbox at the bottom of the Enterprise Voice Port Statistics window.

Voice Port Statistics Counters

To select a set of statistics to display, click one of the option buttons on the lower right-hand corner of the window. The statistics sets are:

- **Packets** - Counters for selected packet types for each IP telephone.
- **Bandwidth** - The rate at which traffic is entering and exiting each IP telephone.
- **Utilization** - The utilized capacity of each IP telephone.

The counters relevant to the selected set of statistics appear under the graph. Check the counters you want displayed. Statistics for the checked counters are displayed as bar graphs.

The following table lists the Voice Port Statistics counters in the Packets statistics set.

Table 5-2. Voice Port Statistics Counters - Packets

Counter	Description
Uncsts Pkts	The number of good unicast packets entering the IP telephone.
Bdcsts Pkts	The number of good broadcast packets entering the IP telephone.
Mcsts Pkts	The number of good multicast packets entering the IP telephone.
Errors In	The number of error packets filtered out by the IP telephone.
Collisions	The number of collisions occurring on the IP telephone.
Good Pkts Out	The number of good packets leaving the IP telephone.

The following table lists the Voice Port Statistics counters in the Bandwidth statistics set.

Table 5-3. Voice Port Statistics Counters - BandWidth

Counter	Description
In BW	The rate at which traffic is entering the IP telephone in Kbps.
Out BW	The rate at which traffic is exiting the IP telephone in Kbps.

The following table lists the Voice Port Statistics counters in the Utilization statistics set.

Table 5-4. Voice Port Statistics Counters - Utilization

Counter	Description
Util	The average percentage of the IP telephone's capacity utilized during the last polling interval.

Sorting the Display

You can sort the display by the device name or any of the counters available for the IP telephone.

To sort the display:

1. Click . The display is sorted by the selected criteria.
2. Select a sorting criterion from the Sort By pull-down listbox.

When sorting by Name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

Searching for IP Telephones

The Find option allows you to locate a specific IP telephone in the Voice Port Statistics window.

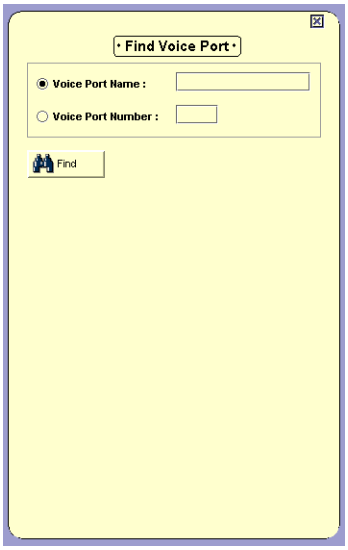
To search for a IP telephone:

1. Click .

   Or

   Select **Edit** > **Find**. The Find IP telephone dialog box opens.

Figure 5-3. Find IP Telephone Dialog Box



2. Enter the IP telephone's IP address in the IP Telephone Name field.

*** Note:** If you enter only part of the IP address, SMON will find the first time the value appears.

3. Click **Find**. The found IP telephone is highlighted for easy identification.

To remove the highlight from the application window, click in the Voice Port Statistics window. The highlight disappears.

*** Note:** The Find button changes to Find Next until all instances of the search information have been found.

6 Introduction to SMON History

This chapter provides an introduction to SMON History, and contains the following sections:

- **Accessing SMON History** - Instructions on accessing the SMON History window.
- **The SMON History User Interface** - A detailed description of the SMON History user interface.
- **Managing Windows** - Instructions on managing SMON History windows.
- **History Text Report** - Instructions on generating a text report on SMON history.

Accessing SMON History

To access SMON History, click the **History** tab in the Avaya SMON Manager window. SMON History opens.

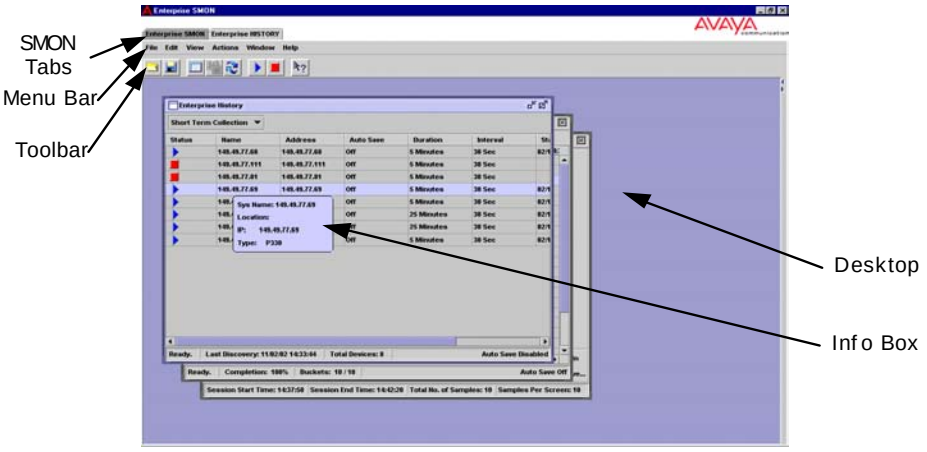
The SMON History User Interface

The user interface consists of the following elements:

- **SMON Tabs** - Tabs providing a method for switching between Online SMON and SMON History.
- **Menu Bar** - Menus for accessing SMON History functions. For information on the full menu structure in SMON History, refer to "SMON History Menus" on page 79.
- **SMON History Toolbar** - Buttons providing shortcuts to important functions in SMON tools.
- **Desktop** - A resizeable window where SMON History windows are displayed.
- **Info Box** - A pop-up box containing information about the item over which the cursor is placed.

The figure below shows the user interface, with its various parts labeled.

Figure 6-1. SMON History User Interface



SMON Tabs

The SMON tabs provide a method for switching between the Online SMON window and the SMON History window. To select a window to view, click the appropriate SMON tab. The relevant window appears.

SMON History Toolbar

The Toolbar provides shortcuts to the main SMON History functions and tools. The following table describes the buttons on the toolbar and lists the equivalent menu options.

Table 6-1. SMON History Toolbar Buttons

Button	Description	Menu
	Opens a saved collection.	**File > Open**
	Saves the SMON History table to a text file.	**File > Save As**
	Uploads the selected collection to the management station.	**View > Switch History**
	Opens a port chart window for the selected port.	**View > Port Chart**
	Refreshes the information in the History Table.	**View > Refresh**

Table 6-1. SMON History Toolbar Buttons (Continued)

Button	Description	Menu
	Activates the selected history collection for the selected devices.	**Actions > Start Collection**
	Deactivates the selected history collection for the selected devices.	**Actions > Stop Collection**
	Opens context sensitive on-line help.	**Help > Help On**

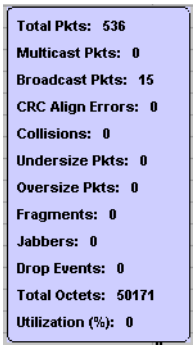
Desktop

The application window is the Desktop. SMON History windows can be resized and minimized. Minimized windows are displayed at the bottom of the Desktop.

Info Box

Info boxes provide information about a device, collection, or point on a Port Chart. When the cursor is placed over a device in the History Table, a port in a History Collection, or a point in a Port Chart for about 2 seconds, an Info Box opens.

Figure 6-2. Info Box



To close the Info Box, move the mouse.

When the cursor is placed over a device in the History Table, the Info Box provides the device's name, location, IP address, and type.

When the cursor is placed over a statistic in a History Collection, the Info Box provides all the counters on the port for the selected interval.

When the cursor is placed over a point in a Port Chart, the Info Box displays the counter, counter value, and time for the selected point.

To toggle the display of Info Boxes, select **View > Info Box**. The display of Info Boxes is toggled.

Managing Windows

When using SMON History to view collections, you may have a large number of open windows. SMON History enables you to manage open windows easily.

To cascade all open windows, select **Window > Cascade**.

To bring the next window in the list to the front, select **Window > Next**.

To bring the previous window in the list to the front, select **Window > Previous**.

To close all windows other than the Enterprise History window, select **Window > Close All**.

*** Note:** The Enterprise History window cannot be closed.

To bring a window in the list to the front, select **Window >** *Window Name*, where *Window Name* is the name of the window you want to view.

History Text Report

The History server saves a text report for every managed device after each Auto-Upload operation. The server creates a separate directory for each device (identified by IP address) and saves all reports generated for the device in this directory. Each day, a new subdirectory is generated in each device's directory (identified by date), and the report for that day is saved there.

The extension of the text report is **`.csvhis`**.

To read a text report, open any standard text editor and open the file you wish to read.

7 Using SMON History

This chapter provides information on how to use SMON History to monitor the traffic on your network, and includes the following topics:

- **Using Enterprise History** - An explanation of the information in the Enterprise History window and instructions on how to use Enterprise History.
- **Using Switch History** - An explanation of the Switch History window and instructions on how to use Switch History.
- **Using Port History** - An explanation of the Port History Chart and instructions on modifying the display.

For a detailed overview of SMON Enterprise History, refer to "Enterprise History" on page 11.

Using Enterprise History

This section provides information about using Enterprise History, and includes the following topics:

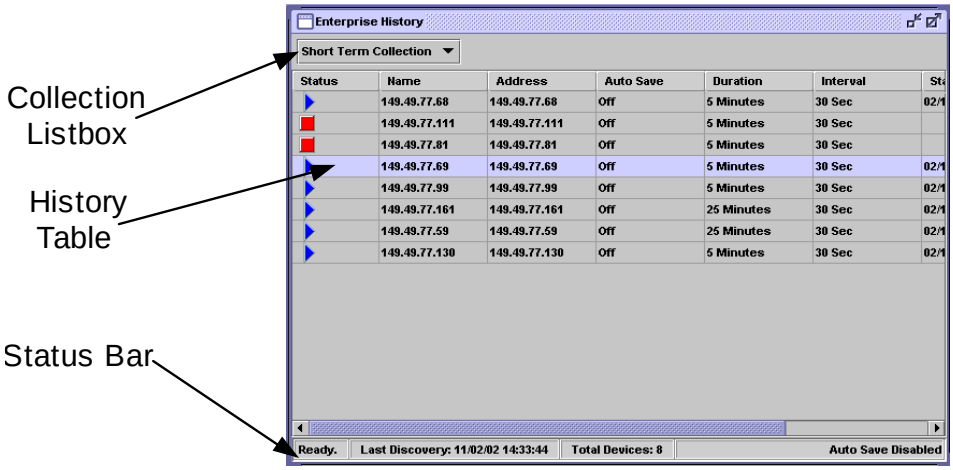
- Understanding the Enterprise History Window
- Collection Parameters
- Activating/Deactivating History Collections
- Activating Auto Save
- Refreshing the Device List
- Saving the Enterprise History Window

Understanding the Enterprise History Window

The Enterprise History window provides a list of supported devices in the network, their collection parameters, and Auto Save status.

The Enterprise History window appears when SMON History opens and cannot be closed while SMON History is running.

Figure 7-1. Enterprise History Window



The Collection Listbox enables you to select the collection type you want to see and configure in the Enterprise History window. The available collection types are Long Term and Short Term Collections.

The following table provides a list of the columns in the History Table and their descriptions.

Table 7-1. History Table Fields

Column	Description
Status	The status of the selected collection. Possible statuses are: - The selected history collection is active. - The selected history collection is inactive.
Name	The device name.
Address	The device's IP address.
Auto Save	Indicates if this collection participates in the Auto Save scheme (**On**) or not (**Off**). For more information, refer to "Activating Auto Save" on page 66.
Duration	The total collection duration time.
Interval	The sampling interval for this collection, i.e., how often the device collects the History data for this Collection.
Started	The date and time when this Collection was started on the device. This field is empty if the Status is inactive.
Last Auto Save	The date and time of the last automatic save of this Collection from the device. If the save was not successful, an error indicator appears. This field is updated with every Auto Save performed on this Collection. It is applicable only if the Collection is active and Auto Save policy is active on the device. For more information, refer to "Activating Auto Save" on page 66.

The following table provides a description of the information displayed in the Enterprise History status bar.

Table 7-2. Enterprise History Status Bar

Item	Description
Discovery Status	The discovery status of SMON History. When Enterprise History is learning the network devices, a progress bar is displayed. When SMON History finishes learning the network devices, **Ready** is displayed.

Table 7-2. Enterprise History Status Bar (Continued)

Item	Description
Last Discovery	The date and time of the most recent discovery.
Total Devices	The number of devices listed in the History Table.
Auto Save Status	Indicates the Auto Save Status. If Auto Save is off for all devices, the Auto Save Status is **`Disabled`**. If Auto Save is active on one or more devices, the Auto Save Status is **`Enabled`**. For more information on Auto Save, refer to "Activating Auto Save" on page 66.
Communication Status	When SMON History is learning the network devices, the following icon is displayed:

Collection Parameters

Each product family, such as the Avaya P130 or Avaya P882 Device, is assigned certain predefined collection parameters. The collection parameters consist of the duration of the collection, the interval at which information is collected, and the number of buckets in the collection. The following table shows the short term and long term collection parameters for different device types:

Table 7-3. Collection Parameters

Device Type	Buckets/ Collection	Short Term Collection		Long Term Collection	
Parameter		**Duration**	**Interval**	**Duration**	**Interval**
P330/P130/C360/G250/G250-BRI/ G350/W310	10	5 min.	30 sec.	5 hrs.	30 min.
P580/P882	50	25 min.	30 sec.	25 hrs.	30 min.
M770	360	1 day	4 min.	14 days	56 min.

*** Note:** It is possible for a collection to contain more than the number of buckets listed above. This occurs when the device saves a new bucket during the upload process. The collection includes all information saved on the device at the time the upload starts and any information added during the upload.

Select a collection type using the Collection pull-down listbox at the top of the Enterprise History window. Collection parameters for the selected collection type are displayed in the History Table.

Activating/Deactivating History Collections

To activate the history collection for one or more devices:

1. Select the devices whose collections you want to activate.

   — To select all the devices in the Enterprise History Table, select **Edit > Select All**.

2. Select a collection type using the Collection listbox at the top of the Enterprise History window.

3. Click in the SMON History toolbar.

   Or

Select **Actions > Start Collection**. The selected collection is activated for the chosen devices.

To deactivate the history collection for a device or several devices:

1. Select the devices whose collections you want to deactivate.

   — To select all the devices in the Enterprise History Table, select **Edit > Select All**.

2. Select a collection type using the Collection listbox at the top of the Enterprise History window.

3. Click in the SMON History toolbar.

   Or

   Select **Actions > Stop Collection.** The selected collection is deactivated for the chosen devices.

If a collection is already active, reactivating or stopping it results in the loss of data collected and stored in the device. A warning dialog box opens with the following options when an active collection is activated or stopped:

- **Yes** - Reactivate/stop the collection.
- **No** - Skip the current device and continue operation for the remainder of the selected devices.

Activating Auto Save

Enterprise History can save History Collections from devices automatically. If Auto Save is enabled for a device, when a History Collection is completed, it is saved to a file. The filename consists of the device name, collection type, date, and time separated with underscores. History Collection files have an **`HIS`** extension.

For example, a file named **`153.34.129.64_Short_Collection_02-24-02_13-42.his`** contains the Short Term Collection for the device with the IP address 153.34.129.64 that was saved at 1:42 PM on February 24, 2002.

To automatically save History Collections:

1. Select the devices whose collections you want to automatically save.

   — To select all the devices in the Enterprise History Table, select **Edit > Select All**.

2. Select **Actions** > **Auto Save On**. History Collections for the selected devices are saved automatically.

When Auto Save is enabled on a device, the Long Term and Short Term Collections are saved automatically.

CAUTION

Auto Save automatically creates reports and saves them to the network management station (NMS). If Auto Save is enabled on many devices for a long period of time, and none of the files are deleted, the NMS's hard disk may become full.

If this occurs, stop the applications that are generating automatic reports and delete the files that are not required.

To stop automatically saving History Collections:

1. Select the devices whose collections you do not want saved automatically.

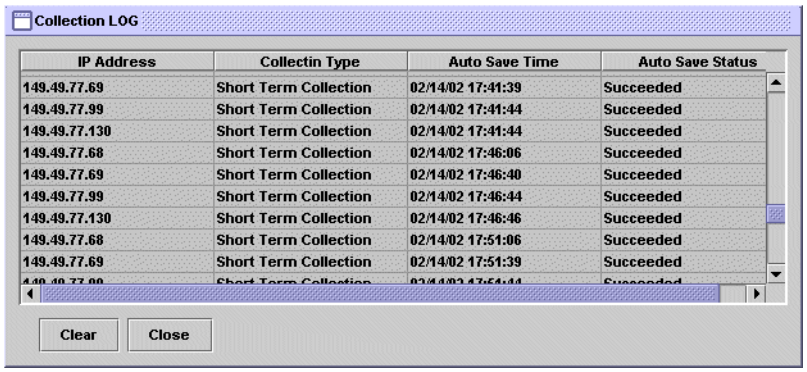
   — To select all devices in the History Table, select **Edit** > **Select All**.

2. Select **Actions** > **Auto Save Off**. History Collections for the selected devices are no longer saved automatically.

Viewing the Collection Log

The Collection Log provides information about History Collections being saved automatically. To view the Collection Log, select **View** > **Collection Log**. The Collection Log opens.

Figure 7-2. Collection Log


Collection LOG
IP Address
Collectin Type
Auto Save Time
Auto Save Status
149.49.77.69 Short Term Collection 02/14/02 17:41:39 Succeeded
149.49.77.99 Short Term Collection 02/14/02 17:41:44 Succeeded
149.49.77.130 Short Term Collection 02/14/02 17:41:44 Succeeded
149.49.77.68 Short Term Collection 02/14/02 17:46:06 Succeeded
149.49.77.69 Short Term Collection 02/14/02 17:46:40 Succeeded
149.49.77.99 Short Term Collection 02/14/02 17:46:44 Succeeded
149.49.77.130 Short Term Collection 02/14/02 17:46:46 Succeeded
149.49.77.68 Short Term Collection 02/14/02 17:51:06 Succeeded
149.49.77.69 Short Term Collection 02/14/02 17:51:39 Succeeded
Clear
Close

The Collection Log contains the following fields:

- **IP Address** - The IP address of the device for which the History Collection was saved.
- **Collection Type** - The type of History Collection saved - Long Term or Short Term.

- **Auto Save Time** - The date and time at which the History Collection was saved.
- **Auto Save Status** - The status of the Auto Save action for the History Collection. If the Auto Save was successful, the Auto Save Status is **Succeeded**. If the Auto Save was not successful, the Auto Save Status contains the reason for the failure.

You can save the Collection Log to a comma separated value (CSV) file. This file can then be imported into a spreadsheet or database program.

To save the Collection Log to a CSV file:

1. Click .

   Or

   Select **File** > **Save As**. A file browser opens.

2. Enter a name for the file in the File name field.

*** Note:** The extension for the filename is **csv**.

3. Browse to the directory in which you want to save the file.
4. Click **Save**. The file is saved.

To clear the Collection Log, click **Clear**. The Collection Log is cleared.

To close the Collection Log, click **Close**. The Collection Log closes.

Refreshing the Device List

You can refresh the list of devices in the Enterprise History window. This is useful after network devices are added to or removed from the network.

To refresh the list of devices in the Enterprise History window:

Click .

Or

Select **View** > **Refresh**. SMON History relearns the devices in the network and refreshes the device list in the Enterprise History window.

Saving the Enterprise History Window

You can save the information in the Enterprise History window to a comma separated value (CSV) file. This file can then be imported into a spreadsheet or database program. To save the Enterprise History window to a CSV file:

1. Click .

   Or

   Select **File > Save As**. A file browser opens.

2. Enter a name for the file in the File name field.

*** Note:** The extension for the filename is **csv**.

3. Browse to the directory in which you want to save the file.
4. Click **Save**. The file is saved.

Using Switch History

This section provides information about using the Switch History window, and includes the following topics:

- Opening a Switch History Window
- Understanding the Switch History Window
- Saving a Switch History Report

Opening a Switch History Window

The Switch History window provides a table with traffic statistics for all of the ports on a selected device. You can upload the Switch History data from a device or open an existing History file. In addition, you can also save the information in a Switch History window to a file.

To upload data from a device to a Switch History window:

1. Select the History Collection to upload using the Collection pull-down listbox.
2. Select the devices whose History Collections you want to upload from the History Table.
   - To select all the devices in the History Table, select **Edit > Select All**.
3. Click .

   Or

   Select **View > Switch History**. A Switch History window opens for each device selected.

To open a saved History file:

1. Click .

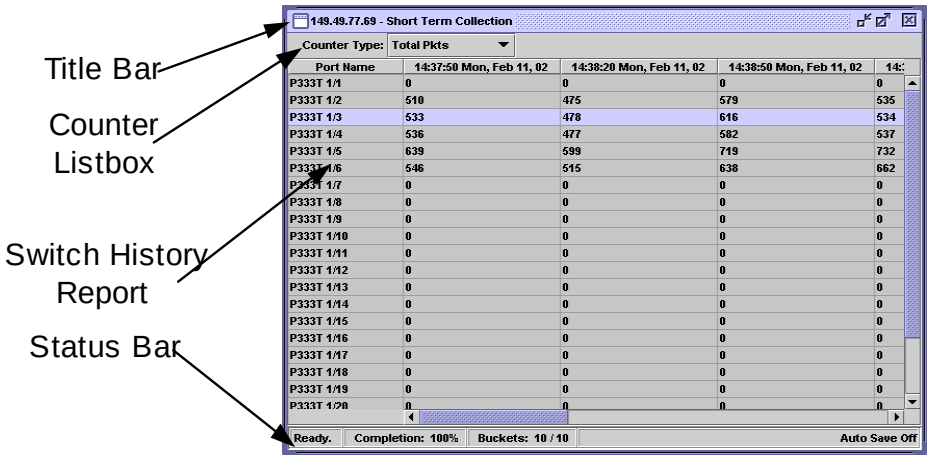
   Or

   Select **File > Open**. A file browser opens.
2. Select an **`his`** file to open.
3. Click **Open**. The selected History file opens in a Switch History window.

Understanding the Switch History Window

The Switch History window provides a list of ports on the selected device, their collection parameters, and Auto Save status.

Figure 7-3. Switch History Window



The Title Bar of the Switch History window provides the following information:

- For uploaded data - The device name and collection type.
- For saved data - The filename of the saved collection.

The Counter Type pull-down listbox enables you to select the counter you want to see in the Switch History Report. The following table provides a list of available counters and their descriptions:

Table 7-4. Switch History Counters

Counter	Description
Total Pkts	The total number of packets entering the switch.
Multicast Pkts	The number of good multicast packets entering the switch.
Broadcast Pkts	The number of good broadcast packets entering the switch.
CRC Align Errors	The number of packets with CRC alignment errors entering the switch.

Table 7-4. Switch History Counters (Continued)

Counter	Description
Collisions	The number of collisions occurring on the switch.
Undersize Pkts	The number of undersize packets entering the switch.
Oversize Pkts	The number of oversize packets entering the switch.
Fragments	The number of packet fragments entering the switch.
Jabbers	The number of jabbers entering the switch.
Drop Events	The number of dropped events on the switch.
Total Octets	The total number of octets entering the switch.
Util (hundredth%)	The percentage of the switch's bandwidth being used.

Each row in a Switch History Report represents a port on the selected device. The first column in a Switch History Report provides port names. Subsequent columns provide the amount of the selected counter at the time and date in the column header. The number of columns in a Switch History Report is one more than the number of buckets in the collection.

The following table provides a description of the information displayed in the Switch History Status Bar.

Table 7-5. Switch History Status Bar

Item	Description
Upload Status	The upload status of Switch History. When Switch History is uploading data from the device, a progress bar is displayed. *** Note:** The upload progress can be greater than 100%. This occurs when the device saves a new bucket during the upload. The uploaded data includes all information saved on the device at the time the upload starts and any information added during the upload. However, the Upload Status percentage is based on the standard number of buckets in the collection. When Switch History finishes uploading data, **`Ready`** is displayed. If the data in the Switch History Report is from a saved file, **`Saved Session`** is displayed.
Completion	The percentage of the Collection that appears in the Switch History Report.
Buckets	The number of buckets in the collection.
Auto Save Status	Indicates the Auto Save Status. If Auto Save is off for the device, the Auto Save Status is **`Auto Save Off`**. If Auto Save is active on the device, the Auto Save Status is **`Auto Save On`**. For more information on Auto Save, refer to "Activating Auto Save" on page 66.
Communication Status	When Switch History is uploading data from a device, the following icon is displayed:

Saving a Switch History Report

You can save the information in a Switch History Report to a history file. This is useful if you manually uploaded a collection, and you want to save it.

To save a Switch History Report to a file:

1. Click .

   Or

   Select **File** > **Save As**. A file browser opens.

2. Enter a name for the file in the File name field.

*** Note:** The extension for the filename is **`his`**.

3. If you want to save the file in a different directory, browse to the directory in which you want to save the file.

4. Click **Save**. The Switch History Report is saved to the file.

Using Port History

This section provides information about using the Port History Chart, and includes the following topics:

- Opening the Port History Chart
- Understanding the Port History Chart
- Modifying the Port History Display

Opening the Port History Chart

The Port History Chart provides a chart with traffic statistics for a selected port. To open the Port History Chart for a port:

1. Select a port from a Switch History Report.

2. Click .

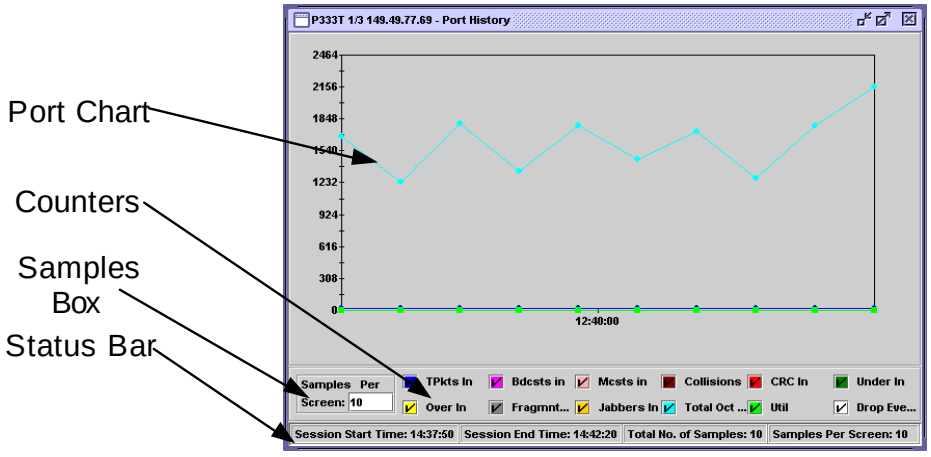
   Or

   Select **View** > **Port Chart**. The Port History Chart opens with information on the selected port.

Understanding the Port History Chart

The Port History Chart provides a graphical representation of the traffic on the selected device during the selected collection.

Figure 7-4. Port History Chart



The Port Chart shows the traffic on the port during the period of the collection. Each counter is represented by a line of a different color.

The Counters checkboxes enable you to select the counters you want displayed in the Port Chart. To view a counter in the Port Chart, check the counter's checkbox.

The Samples Box enables you to configure the number of samples visible in the Port Chart. To configure the number of samples visible in the Port Chart:

1. Enter a number in the Samples Per Screen field.

*** Note:** The number of samples must be between 1 and the number of buckets in the collection.

2. Press **ENTER**. The display changes, showing the selected number of samples in the Port Chart.

The following table provides a description of the information displayed in the Port History Chart Status Bar.

Table 7-6. Port History Chart Status Bar

Item	Description
Session Start Time	The time at which the current Collection started.

Table 7-6. Port History Chart Status Bar (Continued)

Item	Description
Session End Time	The time at which the current Collection ended.
Total No. of Samples	The number of buckets in the collection.
Samples Per Screen	The number of samples visible in the Port Chart.

Modifying the Port History Display

You can modify the display of the Port History Chart.

To compress the graph to show all of the samples in the collection, double-click anywhere in the Port Chart. The Port Chart displays all of the samples in the collection.

To zoom in on the graph, press **SHIFT** and select a portion of the graph using the mouse. The graph zooms in and displays the selected portion.

To return the graph display to the configured number of samples per screen, click anywhere in the Port Chart. The display returns to the configured number of samples per screen.

A Avaya SMON Manager Menus

This appendix provides the full structure of the menus in Avaya SMON Manager.

Online SMON Menus

This section gives the full structure of the menus in the Online SMON page of Avaya SMON Manager.

File Menu

Table A-1. Enterprise SMON - File Menu

Item	Description
New > Switch Statistics	Opens or activates the Enterprise Switch Statistics window.
New > Port Statistics	Opens or activates the Enterprise Port Statistics window.
New > Voice Port Statistics	Opens or activates the Enterprise Voice Port Statistics window.
Close	Closes the active window.
Auto Report	Opens the Auto Report dialog box.
Report Now	Opens the Report Now dialog box.
Options	Opens the Options dialog box.
Exit	Closes Avaya SMON Manager.

Edit Menu

Table A-2. Enterprise SMON - Edit Menu

Item	Description
Configuration	Opens the Port or Switch Configuration dialog box.

Table A-2. Enterprise SMON - Edit Menu (Continued)

Item	Description
Find	Opens the Find dialog box.

View Menu

Table A-3. Enterprise SMON - View Menu

Item	Description
Customize	Opens the Customize Switch or Port dialog box.
Pause	Stops all polling.
Define VLAN Filter	Opens the Define VLAN Filter dialog box.
Activate VLAN Filter	Toggles the VLAN Filter.
Port Default Naming	Toggles between the display of default port names and user defined port names.
IP Telephone Default Naming	Toggles between the display of default IP telephone names and user defined IP telephone names.
Switch Default Naming	Toggles between the display of default device names and user defined device names.

Window Menu

Table A-4. Enterprise SMON - Window Menu

Item	Description
Cascade	Cascades all open windows.
Next	Brings the next open window in the list to the front.
Previous	Brings the previous open window in the list to the front.
Close All	Closes all windows.
Window Name	Brings the named window to the front.

Help Menu

Table A-5. Enterprise SMON - Help Menu

Item	Description
Contents	Opens the on-line help to the Contents page.
Help On	Activates context-sensitive on-line help.
About Avaya SMON Manager	Opens a window with Avaya SMON Manager version and copyright information.

SMON History Menus

This section gives the full structure of the menus in the SMON History page of Avaya SMON Manager.

File Menu

Table A-6. SMON History - File Menu

Item	Description
Open	Opens a saved History collection.
Save As	Saves the current History collection to a file.
Exit	Closes Avaya SMON Manager.

Edit Menu

Table A-7. SMON History - Edit Menu

Item	Description
Select All	Selects all rows in a table.

View Menu

Table A-8. SMON History - View Menu

Item	Description
Switch History	Uploads the selected collection to the management station.
Port Chart	Opens a chart showing the traffic on the port during the collection period.
Collection Log	Opens the Collection Log.
Refresh	Refreshes the information in the History Table.
Info Box	Toggles the display of info boxes.

Actions Menu

Table A-9. SMON History - Actions Menu

Item	Description
Start Collection	Activates the selected history collection for the selected devices.
Stop Collection	Deactivates the selected history collection for the selected devices.
Auto Save Off	Stops automatic history report saving.
Auto Save On	Starts automatic history report saving.

Window Menu

Table A-10. SMON History - Window Menu

Item	Description
Cascade	Cascades all open windows.
Next	Brings the next open window in the list to the front.
Previous	Brings the previous open window in the list to the front.
Close All	Closes all windows other than the Enterprise History window.
Window Name	Brings the named window to the front.

Help Menu

Table A-11. SMON History - Help Menu

Item	Description
Contents	Opens the on-line help to the Contents page.
Help On	Activates context-sensitive on-line help.
About Avaya SMON Manager	Opens a window with Avaya SMON Manager version and copyright information.

B Setting Up the SMON License

Avaya Network Management does not include a license for using SMON. Instead, a trial version of Avaya SMON Manager is included. This trial version expires 60 days after its first use.

The Avaya SMON Manager (with Avaya Network Management) package contains a license that allows you to use Avaya SMON Manager on a permanent basis. The license is supplied as a separate document in the Avaya SMON Manager (with Avaya Network Management) package.

When launching Avaya SMON Manager before entering a valid license key, a dialog box for entering the license key is displayed. If you purchased the Avaya SMON Manager (with Avaya Network Management), enter the provided license key. This allows unlimited use of Avaya SMON Manager. If you purchased the Avaya Network Management package, press **ENTER**. This allows use of Avaya SMON Manager for 60 days.

In addition, an embedded license is required for Device SMON for Avaya P130, Avaya P330, and Avaya M770 Devices. For more information, refer to the appropriate *Avaya Device SMON User Guide*.

*** Note:** There is no Device SMON for the Avaya G250, Avaya G250-BRI, or Avaya G350 devices. These devices are supported in SMON Manager.

Index

A
Accessing
  History 57
  port statistics 35
  switch statistics 27
  voice port statistics 47
Activating
  history collection 65
Adding
  Auto Save devices 66
Auto Save
  adding devices 66
  policy 12
  removing devices 66
Avaya SMON Manager
  introduction 1
  overview 4
  tools 9
Avaya SMON Manager Guide
  intended readers ix
  organization of this guide ix
  purpose ix

C
Changing
  display mode 20
  polling interval 19
Collection
  Log 67
  parameters 65
Collection, Enterprise History
  definition 12
  duration 13
  long term 12
  short term 12
Configuring
  Auto Save 66
  polling interval 19
Counters
  port statistics 43
  switch statistics 32
  voice port statistics 53
Creating
  groups of ports and LAGs to monitor 38
  groups of switches to monitor 30

D
Deactivating
  history collection 65
Desktop 17, 59
Device
  rediscovery 68
Device SMON
  tools 2
Dialog area 17
Dialog box
  find IP telephones 55
  find ports and LAGs 45
  find switches 34
  IP telephone group configuration 50
  port group configuration 38
  switch group configuration 30
Display mode 20

E
Enterprise
  monitoring 3
Enterprise History
  collections 12
  how it works 12
  overview 11
  window 62
Enterprise Port Statistics
  overview 11
Enterprise SMON History, see History
Enterprise Switch Statistics
  overview 10

F
Filter
  TopN 20, 32, 42, 52
  VLAN 41
Find IP telephone dialog box 55
Find port dialog box 45
Find switch dialog box 34
Finding
  IP telephones 55
  ports and LAGs 45
  switches 34
Format report options 21

G
General options
display mode 20
polling interval 19
Generating
Enterprise reports 22
Global network monitoring 3
Groups
creating port 38
creating switch 30

H
History
accessing 57
activating collections 65
collections 65
deactivating collections 65
managing windows 25, 60
toolbar 58
uploading data 74
user interface 57
History Text Report 60
How to
access port statistics 35
access switch statistics 27
access voice port statistics 47
activate history collection 65
add a device to the Auto Save report 66
configure the polling interval 19
create port groups 38
create switch groups 30
deactivate history collection 65
filter ports and LAGs 40
filter switches 32
filter voice ports 52
find ports and LAGs 45
find switches 34
findIP telephones 55
generate reports 22
manage History windows 25, 60
modify the Port History display 76
rediscover devices 68
remove a device from the Auto Save report 66
resize the desktop 17
resize the dialog area 17
select directory to save reports 21
select IP telephones to poll 50
select ports and LAGs to poll 38
select switches to poll 30
sort IP telephones 54
sort ports 44
sort switches 33
upload data to the management station 74
use dialog box options 21
use display mode option 20
use port statistics 36
use switch statistics 28
use the polling interval option 19
use TopN port filtering 42
use TopN switch filtering 20, 32
use TopN voice port filtering 52
use voice port statistics 48
view the Collection Log 67
work with the Online SMON tools 18

I
Intended users ix
Introduction 1
IP telephones
finding 55

L
LAGs
finding 45
Log
Collection 67
Long term history collection 12

M
MAC layer top-down monitoring 6
Management applications 3
Managing
windows 25, 60
Monitoring
global network 3
multi-tiered 6
switch 3
top-down 6

O
Online SMON
toolbar 16
tools 10
user interface 15
working with the tools 18
Organization of this guide ix
Overview of Avaya SMON Manager 4

P
Policy
Auto Save 12
Polling
interval 19
selecting IP telephones 50
selecting ports and LAGs 38
selecting switches 30
setting interval 19

Port group configuration dialog box 38
Port History
  modifying 76
  overview 13
Port statistics
  accessing 35
  counters 43
  tool 35
  using 36
  window 36
Ports
  filtering the display 40
  finding 45
  TopN filtering 42
Purpose of this guide ix

R
Rediscovering devices 68
Removing
  Auto Save devices 66
Reports
  format options 21
  generating 22
  selecting a directory 21
Resizing
  desktop 17, 59
  dialog area 17
RMON standard 1

S
Saving reports 21
Searching
  IP telephones 55
  ports and LAGs 45
  switches 34
Selecting
  directory to save reports 21
  IP telephones to poll 50
  ports and LAGs to poll 38
  report formats 21
  switches to poll 30
SMON
  applications 3
  devices 5
  probes 5
  standard 2
  tabs 16, 58
  tools 3, 9
  top-down monitoring 6
Sorting
  IP telephones 54
  ports 44
  switches 33
Switch group configuration dialog box 30
Switch monitoring 3
Switch statistics
  accessing 27
  counters 32
  tool 27
  using 28
  window 28
Switches
  filtering the display 32
  finding 34
  TopN filtering 20, 32

T
Tool
  port statistics 35
  SMON history 61
  switch statistics 27
  voice port statistics 47
Toolbar
  history 58
  Online SMON 16
Toolbar buttons 16
Tools
  Device SMON 2
  Online SMON 10
Top-down monitoring
  MAC layer 6
  overview 6
  upper layers 7
TopN
  port filtering 42
  switch filtering 20, 32
  voice port filtering 52

U
Understanding
  the port statistics window 36
  the switch statistics window 28
  the voice port statistics window 48
Uploading data to the management station 74
Upper layers top-down monitoring 7
User interface
  desktop 17, 59
  dialog area 17
  Online SMON 15
Using
  Auto Save 66
  dialog box options 21
  port statistics 35, 36
  switch statistics 27, 28
  voice port statistics 47, 48

V
Viewing
  the Collection Log 67
VLAN filter dialog box 41
VLAN filtering 41
Voice port
  group configuration dialog box 50
Voice port statistics
  accessing 47
  counters 53
  tool 47
  using 48
  window 48
Voice ports
  filtering the display 52
  TopN filtering 52

W
Welcome to Avaya SMON Manager ix
What is RMON? 1
What is SMON? 2
Who should use this guide ix
Window
  Enterprise History 62
Windows, managing 25, 60
Working with SMON tools 18